COMMENTS OF THE
AMERICAN PUBLIC POWER ASSOCIATION

Pursuant to the Request for Comments set out in the Federal Register, the American Public Power Association ("APPA") hereby provides comments to the National Institute of Standards and Technology ("NIST") on the "Draft NIST Interagency Report 7628, Smart Grid Cyber Security Strategy and Requirements" ("Report").

I.

APPA'S INTERESTS

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power systems provide over 15 percent of all kilowatt-hour ("kWh") sales to ultimate customers, and do business in every state except Hawaii. Approximately 1,840 of these systems are cities and municipal governments that currently own and control the day-to-day operation of their electric utility systems. Collectively, public power systems serve 45 million people. While some public power systems serve major metropolitan areas, most public power entities serve smaller communities. The median public power system serves approximately 2,000 customers. A typical system of this size has about 10 employees.

1 74 Fed. Reg. 52,183 (October 9, 2009).
All APPA utility members are Load-Serving Entities (“LSEs”), with the primary goal of providing retail electric customers in the communities they serve with reliable electric power and energy at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of APPA-member electric utilities with the long-term interests of the residents and businesses in their communities.

II. COMMENTS

APPA appreciates the hard work and analysis that NIST put into the drafting of the Report. APPA files these comments to assist the drafters as they revise the Report, to ensure that the resulting work product will work for all segments of the industry as cyber security standards are implemented.

APPA has been concerned throughout the NIST standards development process to date that the standards and protocols developed work “on the ground” for all segments of the electric utility industry, including consumer-owned public power systems, many of which are smaller electric utilities. It is easy for the concerns of these industry segments to get lost in the shuffle, since they often do not have the human and technical resources to devote to NIST’s standard-drafting processes. However, consumer-owned utilities (public power systems and rural electric cooperatives) together serve 27 percent of the nation’s electric consumers. NIST therefore needs to build sufficient flexibility into its cyber security requirements to accommodate the sizes and business models of consumer-owned systems.

Section 1.4.1, Selection of use cases with cyber security considerations.

In this section of the Report, the selection of Use Cases is discussed. The Use Cases themselves are set out in Appendix A. APPA comments on Appendix A below;
suffice it to say here that the Use Cases need to take sufficient account of the privacy of customer information, and to accommodate a variety of business models.

**Privacy and the Smart Grid**

**Section 2.2, Summary of [Privacy Impact Assessment (PIA)] Findings**

APPA agrees with NIST that the lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with smart grid management and information collection and use creates a privacy risk that needs to be addressed. Report at 8. Given the very substantial stimulus funds the Department of Energy has recently awarded for various smart grid proposals, it will be necessary in the very near future to address the privacy of customer information generated by smart grid installations. In doing so, regulators and the industry will have to weigh carefully the optimal combination of security measures and the consequences for a breach of privacy information.

APPA notes that some state regulators and their staff see the privacy of customer information as a, if not the, top priority issue associated with smart grid installations. At the recently concluded Winter Meeting of the National Association of Regulatory Utility Commissioners (“NARUC”), held on November 15–18, 2009, in Chicago, the NARUC Committee on Critical Infrastructure voted out Resolution No. CI-1, entitled “Resolution Regarding Cybersecurity and Privacy Issues Surrounding Smart Grid.” This resolution expressed strong concerns about the possibility that private customer data could be shared, misused, stolen or otherwise not adequately protected during smart grid program deployments. In particular, it expressed concerns that third-party access to consumer data, particularly access to real-time usage information, could “pose a physical threat to the consumer as third parties could monitor behavior patterns, such as whether a resident
is home.” The resolution called for the “highest levels” of consumer protections and cyber security. It further called upon NARUC to “recommend federal legislation on cybersecurity and privacy issues be enacted as soon as possible that would put enforcement mechanisms in place that would ensure that any misuse or improper disclosure of consumer data, either intentional or through negligence, would be a federal crime with appropriate sanctions attached.”

This resolution was tabled by NARUC’s Board of Directors, due to concerns expressed about it by certain other NARUC Committees. APPA expects, however, that some form of resolution on these issues will again be considered at the next NARUC meeting, to be held on February 14–17, 2010, in Washington, D.C.

Proposals of this type (especially the possibility of federal criminal liability for even negligent disclosures of customer information) are of substantial concern to APPA. NIST and those drafting cyber security standards under its auspices need to be fully aware of the strong concerns of these state regulators surrounding the privacy of customer information. In response, NIST needs to do two things. First, it needs to ensure that its cyber security standards incorporate into smart grid architecture all reasonable, cost-effective safeguards to protect the privacy of customer information. Second, it needs to educate state and federal policy makers as to the potential costs and benefits of including the “highest level” of cyber security safeguards into smart grid installations.

As Ms. Annabelle Lee of NIST noted in her telephonic presentation on Tuesday, November 17, 2009, at the NARUC Concurrent Session on “The ‘Cyber’ House Rules: What Regulators Need to Know about Cybersecurity,” disclosures of customer data, while certainly unwanted, will be almost inevitable, as meters will be compromised, and it is
virtually impossible to provide 100 percent protection 100 percent of the time from data disclosures. Emphasis on mitigation of such disclosures is therefore appropriate. Further, it could be prohibitively expensive to include the “highest level” of cyber security safeguards into smart grid installations, especially for smaller electric utilities. NIST itself appropriately acknowledges this cost-benefit trade-off in Appendix A at A-3, when it states “[b]alance is also needed between risk and the cost of implementing the security measures.” The combination of very expensive required safeguards and severe punitive measures for even negligent breaches of customer information could be enough to induce many smaller utilities to take a “thanks, but no thanks” attitude to smart grid installations. NIST therefore needs to balance all of these factors in developing its cyber security safeguards, and to educate policy makers about the wisdom of the choices that it makes.

Section 2.3, Purpose of a High-Level PIA

Section 2.5.3, Choice & Consent to use PII

These sections of the Report discuss “personally identifiable information” (“PII”). APPA generally finds the principles for PII set out in Section 2.3 to be reasonable, but notes that if carried out to the fullest extent, some could handicap electric utilities in carrying out their core reliability functions.

Even today, electric utilities provide customer-specific information to third parties in carrying out their utility functions. For example, if there is a customer outage, electric utilities might share that outage information, including specific customer information, with third-party contractors or crews from other electric utilities assisting in the restoration of service. If utilities were required to obtain customer-by-customer consent to such disclosures, their efforts to restore service could be delayed. Since one of the
purposes of smart grid installations is to pinpoint more accurately customer outages, it seems like overkill to require individual customer sign-off on such information disclosures.

On the other hand, APPA certainly understands that PII collected from a customer should not be disclosed without his or her prior permission to vendors or other entities for purposes removed from the utility’s core functions—for example, commercial marketing purposes. APPA’s point is that disclosure requirements should not be so onerous as to interfere with utility service to electric customers.

**Section 2.5.10, Openness, Monitoring and Challenging Compliance**

This section states that “[p]rivacy protections should be applied consistently and at the same level for all PII throughout the entire Smart Grid system to be effective.” Report at 14. APPA is concerned that this concept, if applied literally, could require a small consumer-owned utility to implement all of the same privacy protections for PII that the largest of investor-owned utilities would employ, regardless of the cost of the necessary systems and the personnel to maintain such safeguards. A “rule of reason” will have to be applied, or the perverse result would be that consumers served by smaller utilities will not have access to smart grid technology. While all utilities should implement appropriate safeguards for PII, those safeguards do not necessarily have to be at the same level to be effective.

**Chapter 4, AMI Security Requirements**

This section of the report gives an “initial set” of AMI security requirements. APPA assumes these requirements will be developed further and the final list may become standards that utilities may need to comply with. Therefore, APPA recommends that the requirements be clear, non-prescriptive, cost effective and scalable based on the
criticality of the device or system. The following comments are to assist the drafting team in creating achievable requirements.

APPA commends the Cyber Security Coordination Task Group ("CSCTG") for including suggestions for best practices on policy, procedures, document management, continuity of operations and compliance. However, the focus of these requirements should be on smart grid cyber security. The following requirements from Chapter 4 are better suited for a guidance document in support of these requirements; APPA therefore requests that they be excluded from the final requirements section:

DHS-2.9.1 Information and Document Management Policy and Procedures
DHS-2.9.6 Information and Document Classification
DHS-2.9.9 Information and Document Management Review
DHS-2.10.6/ NIST SP 800-53 MA-2 Periodic System Maintenance
DHS-2.12.1/ NIST SP 800-53 IR-1 Incident Response Policy and Procedures
DHS-2.12.2/ NIST SP 800-53 CP-1 Continuity of Operations Plan
DHS-2.12.4/ NIST SP 800-53 IR-2 Incident Response Training
DHS-2.12.5/ NIST SP 800-53 CP-4, IR-3 Continuity of Operations Plan Testing
DHS-2.12.7/ NIST SP 800-53 IR-4 Incident Handling
DHS-2.12.9/ NIST SP 800-53 IR-6 Incident Reporting
DHS-2.12.10/ NIST SP 800-53 IR-7 Incident Response Assistance
DHS-2.12.11/ NIST SP 800-53 PE-6 Incident Response Investigation and Analysis
DHS-2.12.12/ NIST SP 800-53 CP-4 Corrective Action
APPA believes that a utility must create a culture of cyber security awareness within the organization and the best way to accomplish that is through strong internal policies and procedures. Having a clear division between requirements for smart grid system functionality and the process to secure those systems would help utilities understand the requirements. The following is a non-exhaustive list of those
requirements that APPA feels may be key policies and procedures for inclusion in a System Security Management requirement, similar to the North American Electric Reliability Corporation ("NERC") CIP-007 Standard:

- DHS-2.8.1/ NIST SP 800-53 SC-1 System and Communication Protection Policy and Procedures
- DHS-2.8.8/ NIST SP 800-53 SC-8 Communication Integrity
- DHS-2.8.9/ NIST SP 800-53 SC-9 Communication Confidentiality
- DHS-2.8.11/ NIST SP 800-53 SC-12 Cryptographic Key Establishment and Management
- DHS-2.8.19/ NIST SP 800-53 SA-9 Security Roles
- DHS-2.9.2 Information and Document Retention
- DHS-2.9.3/ NIST SP 800-53 MP-1 Information Handling
- DHS-2.9.8 Information and Document Destruction
- DHS-2.10.1/ NIST SP 800-53 MA-1 System Maintenance Policy and Procedures
- ASAP-2.10.7/ NIST SP 800-53 MA-3 Field Tools
- DHS-2.10.8/ NIST SP 800-53 MA-5 Maintenance Personnel
- DHS-2.10.9/ NIST SP 800-53 MA-4 Remote Maintenance
- DHS-2.12.8/ NIST SP 800-53 IR-5 Incident Monitoring
- DHS-2.14.9/ NIST SP 800-53 SI-9 Information Input Restrictions
- DHS-2.15.1/ NIST SP 800-53 AC-1 Access Control Policy and Procedures
- DHS-2.15.2/ NIST SP 800-53 IA-2 Identification and Authentication Policy and Procedures
- DHS-2.15.3/ NIST SP 800-53 AC-2 Account Management
- DHS-2.15.5/ NIST SP 800-53 IA-5 Authenticator Management
DHS-2.15.7/ NIST SP 800-53 AC-3 Access Enforcement
DHS-2.15.16 Passwords
DHS-2.15.23/ NIST SP 800-53 AC-17 Remote Access Policy and Procedure
DHS-2.15.24/ NIST SP 800-53 AC-17 Remote Access
DHS-2.15.25/ NIST SP 800-53 AC-19 Access Control for Portable and Mobile Devices
DHS-2.15.26/ NIST SP 800-53 AC-18 Wireless Access Restrictions
DHS-2.15.27/ NIST SP 800-53 AC-20 Personally Owned Information
DHS-2.15.28/ NIST SP 800-53 IA-2, IA-8 External Access Protections
DHS-2.15.29/ NIST SP 800-53 SC-7 Use of External Information Control Systems

APPA recommends careful wording of these requirements so that they cover the cyber functionality, but are not so prescriptive as to limit a utility’s ability to provide innovative, cost-effective solutions to cyber security challenges.

APPA also cautions NIST on using existing standards as minimums for these requirements. For example, DHS-2.8.12.2, Supplemental Guidance, states as follows: “Any cryptographic modules deployed within an AMI system, at a minimum, must be able to meet the Federal Information Processing Standard (FIPS) 140-2.” Report at 63 (emphasis added). Another example is DHS-2.15.14/ NIST SP 800-53 IA-7 Cryptographic Module Authentication: “Must comply with FIPS 140-2[.]” Report at 102. Although APPA feels that the FIPS model is a thorough and useful process for the federal government with its need to cover all hazards, APPA is concerned that it is not a cost-effective standard for the NIST Smart Grid Cyber Security requirements process. The NIST requirements should only recognize the FIPS model as one option available for a
utility to use for compliance with these requirements, and should allow for other methods of compliance, especially for smaller utility systems.

APPA also advises NIST to avoid statements of opinion and confusing language in these requirements; for example: “The use of collaborative computing mechanisms on AMI components is strongly discouraged.” Report at 63. If this is a standard, it cannot be “strongly discouraged.” Similarly, DHS-2.8.8.2, Supplemental Guidance, states: “When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization must either implement appropriate compensating security measures or explicitly accepts the additional risk.” Report at 61. APPA agrees that the use of appropriate compensating security measures should be an option, especially in the case of legacy systems. APPA is confused, however, by the reference to acceptance of additional risk. Does this mean that the standard could be met merely by acceptance of the additional risk? Further clarification of this point is required.

APPA is concerned that DHS-2.8.7.1 Requirement incorporates unclear statements that may be taken as opinion. That standard states: “In AMI, the very concept of boundaries is problematic. Internal systems within the organization may be more easily protected than components which resides outside significant physical boundaries and controls. Meters and poll-top and other systems without significant controls and external monitoring cannot be amply secured and should always be considered relatively untrusted.” Report at 60. This statement assumes that the utility could not mitigate this risk through upgrades in technology, changing of operating procedures or by other means yet to be devised.
The text of DHS-2.8.7.2 Supplemental Guidance acknowledges it is evaluating only the current state in cyber security for this technology: “At this time components and systems connected to the Internet constitute a substantial increase in risk for the core functionality of the AMI system.” (Emphasis added.) This admits that at some future time the use of the internet may be a secure communication path, which therefore should not be categorically excluded from use. Also, some of the text is contradictory. For example, in DHS-2.8.7.2, guidance item #1 it states: “Generally, no AMI system information should be publicly accessible.” However, guidance item #2 states: “The organization must prevent public access into the organization’s internal AMI system networks except as appropriately mediated and monitored[.]” This guidance should not be included unless it is made clear what the organization must do to secure communication paths in order to be in compliance.

APPA advises the drafting team to avoid requirements that dictate “how” to comply with a standard or requirement. Unduly prescriptive requirements curb each utility’s ability to come up with innovative, least-cost options. For example, DHS-2.8.18.2 Supplemental Guidance states: “The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information must be documented, tracked, and audited periodically. After identifying these connection points, the extent of their protection needs to be determined.” Report at 65. APPA recommends that if the drafting team wants to give a list of suggested solutions or guidance, these items should be included in a guideline that supports the requirement, rather than being made part of the requirement.
APPA agrees that it is a good business practice to automate the system maintenance records when there are a significant number of components to check. Doing so, however, should not be a requirement for documentation because it does not enhance the process to secure smart grid systems. For example, DHS-2.10.6.3, Requirement Enhancements, states: “The organization employs automated mechanisms to schedule and conduct maintenance as required and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.” Report at 75 (emphasis added). APPA recommends that the word “automated” be removed from any requirement addressing documentation only. A good example of where “automated mechanisms” should be used is in DHS-2.15.24.3 Requirement Enhancements, which states: “1. The organization shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.” Report at 107. This use of automation enhances the security of smart grid systems.

As a general matter, APPA believes the requirements should be rigorous, but also reasonable and achievable. It is expected that the life cycle of most smart grid devices will be in excess of 30 years, which is typical of other utility assets. It is assumed that the goal for these requirements is the long-term functionality of the smart grid systems and it is the intent to require reasonable records retention that supports this goal. In DHS-2.9.7.2 Supplemental Guidance it states: “The organization shall employ appropriate measures to ensure long-term records information can be retrieved.” and “The organization must take special care to confirm the security, availability, and usability of the AMI components configuration, which includes the logic used in developing the configuration or programming for the life of AMI system.” Report at 71 (emphasis added). APPA is
concerned with the use of terms such as: “long-term” and “life” in these standards and recommends that they be defined so records retention requirements are not unreasonable.

As stated earlier, the median public power system serves approximately 2,000 customers, and a typical system of this size has about 10 employees. These cyber security requirements and the smart grid standards that are a part of this monumental process must apply to large investor-owned utilities and small consumer-owned utilities. With that in mind we ask that NIST evaluate the cost to implement, maintain and document compliance with the requirements that are being developed and weigh that cost against the value or enhancement to security received from implementing that requirement. APPA has compiled a list of component requirements whose enhancement to security does not appear to justify the cost of implementation:

DHS-2.9.10/NIST SP 800-53 AC-15 Automated Marking
DHS-2.15.17/ NIST SP 800-53 AC-8 System Use Notification
DHS-2.15.19/ NIST SP 800-53 AC-7 Previous Logon Notification
DHS-2.16.6/ NIST SP 800-53 AU-6 Audit Monitoring, Analysis, and Reporting
DHS-2.16.7/ NIST SP 800-53 AU-7 Audit Reduction and Report Generation
DHS-2.16.9/ NIST SP 800-53 AU-9 Protection of Audit Information

Although APPA agrees having these features would be helpful, requiring this functionality in every component may increase the cost unnecessarily when a utility policy or procedure may achieve the same or better results for less cost. APPA requests that all requirements that mandate specific functionality should go through a simple cost-benefit analysis.
Similar to the component list above, the following operational requirements, when evaluated by a small utility, would impose significant and redundant costs when compared to the security benefit:

DHS-2.12.13/ NIST SP 800-53 CP-6 Alternate Data Storage Sites: “The organization shall identify an alternate storage site and initiate necessary agreements to permit the storage of software, data, and configuration information for all components of the AMI system.” Report at 81.

DHS-2.12.15/ NIST SP 800-53 CP-6, CP-7, CP-8 Alternate Control Center: “The organization shall identify an alternate control center, necessary telecommunications, and initiate necessary agreements to permit the resumption of the operation of the AMI system within an organization-prescribed time period when the primary control center is unavailable.” Report at 82.

APPA believes for a majority of small utilities these two requirements by themselves would be unattainable and would therefore restrict their ability to install smart grid systems under these standards. APPA suggests that if these requirements must be part of the standards, that alternatives are allowed that do not mandate such costly solutions.

APPA believes that a multitude of possibilities exist to mitigate the never-ending list of vulnerabilities which arise in smart grid interoperability. In order for these requirements to be effective and to assist utilities in focusing on those issues that are most important, APPA recommends that the CSTCG create a tiered approach to smart grid cyber security.
Some examples of requirements that already identify the need for a definition of security levels are:

DHS-2.9.4/ NIST SP 800-53 RA-2 Information Classification: “All information related to AMI components is classified to indicate the protection required commensurate with its sensitivity and consequence.” Report at 70.

DHS-2.15.18/ NIST SP 800-53 AC-10 Concurrent Session Control: “The AMI components limit the number of concurrent sessions for any user on the AMI system based on the criticality level of the component.” Report at 105.

DHS-2.15.20/ NIST SP 800-53 AC-7 Unsuccessful Login Attempts: “The AMI components shall limit the number of consecutive invalid access attempts by a user during a given time period based on the criticality level of the component.” Report at 105.

DHS-2.15.22 Remote Session Termination: “On critical high-risk systems it may also be advised that the ports and/or software applications for remote access must be disabled and in some cases physically disconnected.” Report at 106.

DHS-2.15.24/ NIST SP 800-53 AC-17 Remote Access: “Remote access to the AMI components must be enabled only when appropriate and with a level of authentication appropriate to the criticality of the system.” Report at 107.

A possible metric for this tiered approach is given below:

- Low—(i.e., a meter or single node, a non critical functionality)—Recommended but not required.
- Medium—(i.e., ability to control multiple devices)—Requirement for operationally significant facilities.
- High—(i.e., ability to control critical functionality of all interconnected devices)—Required to follow all steps in the requirement.
This tiered approach is similar to proposals being evaluated by the NERC standards drafting team that is revising the Critical Asset Identification standard CIP-002.

Appendix A

In Appendix A (at A-2), NIST sets out three key security requirements (Integrity, Availability, and Confidentiality) for the Use Cases that follow. NIST then states that “[c]onfidentiality is generally the least critical [security requirement] for actual power system operations, although this is changing for some parts of the power system, as customer information is more easily available in cyber form.” As APPA has noted above, for certain state regulators, confidentiality is of the utmost importance, to the point that they favor federal legislation that would make even negligent breaches of customer information a federal crime. APPA therefore again urges NIST to follow a two-track approach regarding this issue: (1) ensuring that its cyber security standards incorporate into smart grid architecture all reasonable and cost-effective safeguards to protect the privacy of customer information, while also (2) educating state and federal policy makers as to the potential costs and benefits of including the “highest level” of cyber security safeguards into smart grid installations.

Turning to the actual Use Cases, APPA notes with appreciation that certain of the use cases/scenarios, e.g., “Real Time Pricing (RTP) for Customer Load and DER/PEV” (at A-10-11) and “Time of Use (TOU) Pricing” (at A-11-12), specifically state that demand response can be implemented in many different ways, and that rate designs can differ from utility, being either real-time or tariff-based. It is important that the use cases build in such flexibility, so that different rate designs and business models can be fully accommodated.

On the other hand, the “Bulk Power Electricity Market” use case/scenario still appears to assume one form of wholesale power supply market—the centralized markets
run by Regional Transmission Organizations (“RTOs”). This case’s Category Description states (at A-20) that “[t]he market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives.” The Scenario Description states that the “bulk power market varies from region to region and is conducted primarily through Regional Transmission Operators (RTO) and Independent System Operators (ISO).” Id. NIST should be aware that state regulators and legislators in many regions of the country have decided not to implement retail electric industry restructuring or to proceed with RTOs/ISOs at the wholesale level, including the Southeast, Desert Southwest, Mountain West and Pacific Northwest. APPA does not anticipate Order No. 2000-compliant RTOs forming in these regions any time soon. This scenario should therefore be revised to reflect the continuing regional diversity in wholesale power markets.

Similarly, the Retail Power Electricity Market scenario/use case needs to be revised. While the Category Description notes that the electricity market varies significantly from state to state, region to region and at local levels, it goes on to state that “[t]he market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives.” This description fails to take into account current regulatory realities. Many states did move to implement retail restructuring of their electric utilities in the late 1990s, but after the debacle in California, and the failure of retail restructuring over time to fulfill the promise of lower electric rates in many states,
states that had not done so largely decided to “stay put.”\(^2\) This situation shows little signs of changing, although vertically integrated utilities in these regions have shown increasing interest in smart grid installations and time-differentiated rate designs.

Similarly, consumer-owned electric utilities generally did not implement retail restructuring, even if they were located in regions where investor-owned utilities were restructured. These utilities are owned by their consumers and continue to be vertically integrated. Consumer-owned utilities generally see their role as helping their customers manage energy usage, price volatility and overall bills, rather than simply stepping back and letting their retail customers experience the full brunt of volatile wholesale market pricing (whether they want it or not). As noted above, consumer-owned utilities currently serve 27 percent of the United States’ electric consumers. For all of these reasons, the Retail Power Electricity Market use case/scenario needs to be revised to accommodate the full range of retail electric utility business models, rather than assuming an unjustified evolutionary path.

\(^2\) Indeed, at least one state, Virginia, has repealed its retail restructuring legislation. For a recent analysis of retail rates in restructured and traditionally regulated states, see, Retail Electric Rates in Deregulated and Regulated States: 2008 Update, published in March 2009 by APPA, available at http://www.appanet.org/files/PDFs/RKWFinal2008update.pdf
III.

COMMUNICATIONS

APPA requests that any communications in this matter be directed as follows:

Susan N. Kelly  
Vice President of Policy Analysis  
and General Counsel  
American Public Power Association  
1875 Connecticut Avenue, N.W.  
Suite 1200  
Washington, D.C. 20009-5715  
202-467-2933  
skelly@appanet.org

Michael Hyland  
Vice President, Engineering Services  
American Public Power Association  
1875 Connecticut Avenue, N.W.  
Suite 1200  
Washington, D.C. 20009-5715  
202-467-2986  
mhyland@appanet.org

Nathan Mitchell  
Director of Electric Reliability Standards  
and Compliance  
American Public Power Association  
1875 Connecticut Avenue, N.W.  
Suite 1200  
Washington, D.C. 20009-5715  
202-467-2925  
nmitchell@appanet.org
WHEREFORE, APPA submits these comments for NIST’s consideration.

Respectfully submitted,

AMERICAN PUBLIC POWER ASSOCIATION

By /s/ Susan N. Kelly

Susan N. Kelly
Vice President of Policy Analysis
and General Counsel

Michael Hyland
Vice President, Engineering Services

Nathan Mitchell
Director of Electric Reliability Standards
and Compliance

American Public Power Association
1875 Connecticut Avenue, N.W., Suite 1200
Washington, D.C. 20009-5715

(202) 467-2900
Fax: (202) 467-2918
Email: skelly@appanet.org
mhyland@appanet.org
nmitchell@appanet.org

December 1, 2009