751(a)(1) and 777(i) of the Act and 19 CFR 351.221(b)(4).

Dated: April 7, 2010.

Ronald K. Lorentzen,

Deputy Assistant Secretary for Import Administration.

[FR Doc. 2010–8424 Filed 4–12–10; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 100202060–0143–01]

Second DRAFT NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements; Request for Comments

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce.

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) seeks comments on the second draft of NISTIR 7628, *Smart Grid Cyber Security Strategy and Requirements.* This second draft has been updated to address the comments submitted. In addition, the privacy, vulnerability categories, bottom-up analysis, individual logical interface diagrams, and the cyber security strategy sections have all been updated and expanded and the requirements section has been revised to include requirements for the entire Smart Grid. Finally, there are new sections on research and development, standards assessment, and an overall logical functional architecture. This is the second draft of NISTIR 7628; the final version is scheduled to be posted in the spring of 2010.

DATES: Comments must be received on or before June 2, 2010.

ADDRESSES: Written comments may be sent to: Annabelle Lee, National Institute of Standards and Technology, 100 Bureau Dr., Stop 8930, Gaithersburg, MD 20899–8930. Electronic comments may be sent to: *cswgdraft2comments@nist.gov*.

The report is available at: *http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628*.

FOR FURTHER INFORMATION CONTACT: Annabelle Lee, National Institute of Standards and Technology, 100 Bureau Dr., Stop 8930, Gaithersburg, MD 20899–8930, telephone (301) 975–8897.

SUPPLEMENTARY INFORMATION: Section 1305 of the Energy Independence and Security Act (EISA) of 2007 (Pub. L. 110–140) requires the Director of the National Institute of Standards and Technology (NIST) "to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." EISA also specifies that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid: * * *

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.

(2) Dynamic optimization of grid operations and resources, with full cyber-security * * *"

With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information, the information technology (IT) and telecommunications infrastructures have become critical to the energy sector infrastructure.

NIST has established a Smart Grid Interoperability Panel. The Panel's Cyber Security Working Group (SGIP–CSWG) now has more than 375 volunteer members from the public and private sectors, academia, regulatory organizations, and Federal agencies. Cyber security is being addressed in a process that will result in a comprehensive set of cyber security requirements. These requirements are being developed using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid.

NIST published a request for public comments in the **Federal Register** on October 9, 2009 (74 FR 152183) to seek public comment on the first draft of NIST Interagency Report (NISTIR) 7628, *Smart Grid Cyber Security Strategy and Requirements*.

The comment period closed on December 1, 2009. The second draft of NISTIR 7628 incorporates changes based on the comments received, which are summarized below. The complete set of comments and NIST's analysis are posted at: *http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628.*

Summary of Public Comments Received by NIST in Response to the Draft NISTIR 7628, Cyber Security Strategy and Requirements, and NIST's Response to Those Comments

NIST received comments from sixty-three (63) organizations and individuals. The commenters consisted of twenty-three (23) private companies, five (5) Federal agencies, nine (9) individuals, twelve (12) non-profit organizations, twelve (12) industry associations and two (2) universities. A detailed analysis of the comments follows.

General Comments

Comment: Fifteen (15) commenters identified inconsistencies between the text and logical interface diagrams and suggested additions or deletions to the logical interface diagrams and associated text.

Response: In the second draft of NISTIR 7628, the logical interface diagrams and text have been updated and an overall functional logical architecture has been added.

Comment: Fifty-one (51) commenters suggested grammatical, editorial, and language changes and correcting cited information and sources.

Response: The relevant sections were updated to reflect suggested changes. Some suggested changes were not accepted because they are not consistent with Government Printing Office (GPO) style.

Comment: One (1) commenter suggested integration of cryptographically strong identity management mechanisms.

Response: Strong authentication is an important aspect of the Smart Grid. This will be addressed in the next version of the NISTIR. There were several topics that were not addressed in the second draft of the NISTIR. The schedule for completing the second draft was extremely tight. Therefore, we will address this comment in the June draft, which is the next version.

Comment: One (1) commenter suggested that security requirements be amended to address potential insider threats.

Response: The security requirements are intended to address threats from insiders and external entities. For the next version of the NISTIR, additional analysis will be completed to ensure that the insider threat is addressed. There were several topics that were not addressed in the second draft of the NISTIR. The schedule for completing the second draft was extremely tight. Therefore, we will address this comment in the June draft, which is the next version.

Comment: Seven (7) commenters suggested amendments to the definition of the term "cyber security" to be more inclusive of the electric sector.

Response: The definition of "cyber security" was modified to focus on the electric sector.

Comment: Four (4) commenters suggested including definitions of frequently used terms and acronyms to ensure clear and consistent meanings throughout the document.

Response: A glossary has been included in the second draft of the NISTIR.

Comment: Seven (7) commenters recommended establishing regulations and policies addressing various facets of Smart Grid, including naming an enforcement authority, privacy training and awareness, management and user accountability, use and retention of user data, and law enforcement access to Smart Grid data.

Response: These comments are outside the scope of the NISTIR and the Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) because they focus on regulations and policies.

Comment: Eighteen (18) commenters suggested that the NISTIR should be clarified with respect to purpose and intent of the document. It does not create Smart Grid Cyber Security "requirements," rather acts as a strategy document intended to facilitate the development of such requirements.

Response: The NISTIR was revised to clarify that the document is a guidance document and that the content is not mandatory. In addition, text was added to clarify how the NISTIR may be used by organizations as they develop a cyber security strategy and specify security requirements for the Smart Grid.

Comment: Three (3) commenters suggested adding the following sections to the NISTIR:

- Multi-Tier Control System Criticality Model.
- Control System Trust Model.
- Threat-based Requirements.

Response: These comments are being reviewed for possible inclusion in the next version of the NISTIR. There were several topics that were not addressed in the second draft of the NISTIR. The schedule for completing the second draft was extremely tight. Therefore, we will address this comment in the June draft, which is the next version.

Comment: One (1) commenter proposed use of risk-based performance standards rather than security-specific requirements.

Response: The comment will be considered during the development of the next version of the NISTIR. There were several topics that were not addressed in the second draft of the NISTIR. The schedule for completing the second draft was extremely tight. Therefore, we will address this comment in the June draft, which is the next version.

Comment: One (1) commenter encouraged NIST to collaborate closely with the electric utility industry to develop options for integrating legacy equipment into a smarter grid.

Response: The NISTIR has been revised to clarify that the content is at a high level and each organization will need to address security based on their specific requirements. The intent of the NISTIR is to identify security requirements for the end-to-end grid, including the integration of legacy equipment.

Comment: One (1) commenter advised NIST to implement role-based access control to Smart Grid data.

Response: The NISTIR has been revised to include role-based access control because NIST agrees that role-based access control is good practice.

Comment: Four (4) commenters suggested that the NISTIR should focus on the specificity of standards pertaining to cyber security rather than data privacy.

Response: Both reliability and privacy are being addressed by the NISTIR as both are critical to the effective operation of the Smart Grid.

Comment: One (1) commenter recommended creating a risk management framework focused on protecting the functions of the electric power system rather than the individual assets.

Response: The risk assessment process included in the NISTIR addresses the functions of and information in the electric grid, not individual assets.

Comment: One (1) commenter suggested that interoperability and system security standards be developed that apply directly to the interfaces and the equipment being integrated.

Response: This design consideration will be reviewed in depth for the next draft of the NISTIR. There were several topics that were not addressed in the second draft of the NISTIR. The schedule for completing the second draft was extremely tight. Therefore, we will address this comment in the June draft, which is the next version. The NISTIR is intended to assist all stakeholders of the Smart Grid as they develop requirements and integration strategies.

Comment: One (1) commenter recommended assessing any potential cyber security impacts on the Smart Grid beyond the scope of IT and telecommunications; new vulnerabilities applicable to the Smart Grid could be introduced regularly.

Response: The second draft of the NISTIR provides additional information on impacts that affect the reliability of the Smart Grid. The second draft of the NISTIR clarifies that a risk assessment needs to be performed at regular intervals to address new threats and vulnerabilities. This discussion will be further expanded on the next version of the NISTIR.

Comment: Five (5) commenters suggested including a high-level "summary" or user guide of the document in order to help readability.

Response: The final version of the NISTIR will include design considerations and/or a user guide to assist people in the use of the document.

Comment: One (1) commenter inquired about how NIST would evolve the document to address emerging threats, Smart Grid paradigms and other changing elements of security.

Response: The second draft of the NISTIR clarifies that the risk assessment needs to be performed at regular intervals to address emerging threats, new vulnerabilities, and changes in technology. This discussion will be further expanded on the next version of the NISTIR.

Comment: One (1) commenter inquired about Smart Grid Security Certification and NIST's role in determining the relevancy of such certification.

Response: The Smart Grid Interoperability Panel (SGIP) Testing and Certification Committee has been established to focus on this issue. The SGIP–Cyber Security Working Group (SGIP–CSWG) will be coordinating with this new committee.

Comments and Responses Regarding Chapter One, Cyber Security Risk Management Framework and Strategy

Comment: One (1) commenter suggested that the NISTIR document be revised to be consistent with the "NIST Framework and Roadmap for Smart Grid Interoperability Standards." Also, the document should clearly articulate a strategy for Smart Grid Cyber Security.

Response: The cyber security strategy in the NIST Framework and the NISTIR are the same. Also, additional information was included in the NIST Framework document and in the NISTIR to clarify how the two documents should be used.

Comment: One (1) commenter requested a more detailed definition of how the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards 002–CIP 009 will apply to the Smart Grid. These standards currently apply to the bulk power system and it would be costly to apply them to all of the

Advanced Metering Infrastructure (AMI) and Distribution systems.

Response: The NERC CIPs are mandatory for the bulk power system. The NISTIR includes security requirements for the entire Smart Grid, and the NERC CIPs are some of the standards used as source documents for the security requirements.

Comment: Two (2) commenters commented about the aggressive timeline for developing security requirements and the potential for inferior standards, requirements, and/or strategies because of the limited timeline.

Response: Because of the short time schedule, tasks are being done in parallel. The SGIP–CSWG recognizes the impact this may have and is working hard to ensure the quality is at a high level.

Comment: One (1) commenter noted the impact of new logical interface categories, security considerations, and appropriate controls on the current NISTIR. The overview should mention that the document is not exhaustive and excludes certain topics.

Response: The second draft of the NISTIR clarifies that the document is neither finalized nor comprehensive on all topics.

Comment: One (1) commenter proposed two specific strategies for developing a cyber security framework for the Smart Grid:

1. NIST and the industry should develop a focus on response and recovery. Although the primary goal of a cyber security strategy should be prevention, a response and recovery plan needs to be developed in the event of a cyber attack.

2. It is essential that those parts or equipment of the Smart Grid that optimize the system are separate from the core components of the Smart Grid. In the event of a cyber security incident on the grid, the core components can be recovered with minimal technology in a quick and efficient manner, thereby assuring bulk power system reliability. This will also help identify where response plan decisions and actions can be carried out to protect core functionality and/or quickly restore it.

Response: The cyber security strategy included in the NISTIR addresses prevention, response, and recovery for events that affect the Smart Grid. The cyber security strategy and the security requirements included in the NISTIR are at a high level and do not focus on specific parts and equipment. It is the responsibility of each organization to provide more granular security requirements. Also, the NISTIR addresses the entire Smart Grid, not just the bulk power system.

Comment: One (1) commenter suggested the expansion of the risk assessment to address distribution, transmission, and generation, in addition to AMI.

Response: The second draft of the NISTIR clarifies that the risk assessment should address the entire Smart Grid, not just AMI.

Comment: One (1) commenter inquired about the Smart Grid distribution system in relation to the jurisdiction of NERC.

Response: The NISTIR addresses the entire Smart Grid. Any questions related to the jurisdiction of NERC should be forwarded to that organization.

Comment: One (1) commenter recommended a continual assessment of cyber security risks to the Smart Grid be performed. This way, a common lexicon or language to capture system vulnerabilities that require continual monitoring can be determined.

Response: This recommendation will be considered for the final version of the NISTIR.

Comment: One (1) commenter suggested that NIST should integrate adequate cyber security protection at all levels (device, application, network and system) in the development of a cyber security strategy. This level of cyber security protection should go beyond the requirements of NERC CIP Reliability Standards.

Response: The NISTIR has been modified to clarify that the security requirements are applicable to the entire Smart Grid. The NERC CIPs were considered in the development of the security requirements.

Comments and Responses Regarding Chapter Two, Privacy and the Smart Grid

Comment: One (1) commenter suggested that NIST's approach to Smart Grid privacy is insufficient.

Response: The privacy chapter has been significantly revised and includes more comprehensive privacy principles.

Comment: One (1) commenter recommended that fair information practices be adopted.

Response: The second draft of the NISTIR has a rewritten privacy chapter that includes privacy principles that addresses this concern.

Comment: One (1) commenter suggested that a rulemaking be developed so that service providers establish a concrete set of approved purposes for which PII activity is permitted. That list of approved purposes should be very limited and PII activity only be permitted for purposes essential to the functioning of the Smart Grid. Also, restrictions on the use and retention of data should be mandatory, not merely best practices.

Response: The scope of the NISTIR is to provide recommendations. Implementation of regulations and mandatory practices are outside the scope of the NISTIR and the CSWG.

Comment: One (1) commenter stated the importance of having clear, strong language spelling out specific privacy protection.

Response: The privacy chapter of the second draft of the NISTIR has been revised and now includes revised privacy principles relevant to the Smart Grid.

Comment: One (1) commenter suggested that the privacy chapter should relate how the findings in the "high-level privacy impact assessment (PIA) of the consumer-to-utility metering data sharing portion of the Smart Grid" can be applied to the whole of the Smart Grid. Otherwise, this whole chapter belongs as an appendix as a summary of those findings.

Response: The privacy chapter in the second draft of the NISTIR clarifies that the privacy impact assessment was performed for the entire Smart Grid.

Comment: Two (2) commenters recommended removing the privacy chapter from the NISTIR and creating a stand-alone document about Smart Grid Privacy.

Response: Privacy is an important topic and is addressed alongside cyber security in the NISTIR. Although privacy and security are not the same, many of the security requirements that address privacy also address confidentiality which is a security objective. Because the two are closely related, they are both included in the NISTIR.

Comment: One (1) commenter proposed adopting a "privacy by design" approach. By building standards that reflect privacy interests, rather than attempting to tack on privacy at a later point, this is the most effective means of protecting consumer privacy and security. Ensuring privacy is addressed at an early stage will also be less expensive than attempting to address these issues in the future and will make the grid more adaptable to changing threats to privacy and security as use increases.

Response: Organizations utilizing the Smart Grid should take a holistic view toward privacy, building in privacy from project initiation whenever possible, rather than as an add-on at a later date. This will be further expanded in the next draft of the NISTIR. The Privacy sub-group plans to develop

relevant use cases with the intent of including them in the final version of the NISTIR. The second draft of the NISTIR includes suggested privacy principles that are applicable to the Smart Grid that may be useful to many organizations.

Comment: Eight (8) commenters encouraged including privacy principles to cover all Smart Grid entities and practices and develop use cases that reflect a comprehensive model of data flow detailing necessary consumer privacy protections.

Response: The second draft of the NISTIR includes privacy principles applicable to the entire Smart Grid. The next draft of the NISTIR will include privacy use cases.

Comment: Two (2) comments suggested updating the NISTIR to address privacy policies, standards, and supporting procedures on information collection and uses.

Response: The privacy section has been revised to include privacy principles that address these concerns.

Comment: Three (3) commenters suggested that any attempt to define Personally Identifiable Information (PII) must account for rules and definitions of PII in other jurisdictions. There is also a difference between data privacy and data security. NIST should focus on data security issues and especially upon data security that effectively frustrates security breaches that result in identity theft.

Response: In the second draft of the NISTIR the content of the privacy chapter has been revised and the term PII is not included. PII is defined very specifically and does not include concepts that are used in Smart Grid. Both data privacy and data security are important to the Smart Grid and are included in the NISTIR.

Comment: One (1) commenter suggested that it will be necessary to address the privacy of customer information generated by Smart Grid installations.

Response: The privacy chapter has been revised and includes privacy principles.

Comments and Responses Regarding Chapter Three, Logical Interface Analysis

Comment: Twenty-seven (27) commenters recommended changing the impact levels of various logical interface categories.

Response: The impact levels for the logical interface categories have been revised. They will continue to be reviewed and revised for the final version of the NISTIR.

Comment: One (1) commenter proposed two additional constraints to Category 11—

1. System scale and diversity prohibits a unified solution to security management.

2. Ubiquitous networking of devices combined with remote control capabilities can enable coordinated manipulation of load on a large scale.

Also, an additional impact to Category 11 was proposed—

1. Possible large-scale load manipulation through distributed control of unsecured or compromised devices.

Response: The Logical Interface Category Definitions section has been rewritten in the second draft of the NISTIR. Rather than constraints, Table 3.1 provides the analysis matrix of the security-related logical interface categories against the attributes that reflect the interface categories.

Comment: One (1) commenter suggested that the logical interface diagrams be moved and re-titled "Proposed Logical Interfaces."

Response: The second draft of the NISTIR has been revised to clarify that these are logical interface diagrams, are not solutions, and do not imply any architectural implementations.

Comment: One (1) commenter identified a high-risk, low-tech attack that did not apply to the Confidentiality, Integrity, or Availability (CIA) of Smart Grid data.

Response: Both the Vulnerability and Bottom-up sub-groups within the SGIP–CSWG will review this attack to include in Appendix C or Appendix D of the final version of the NISTIR.

Comment: Twenty (20) commenters suggested changes to examples within the logical interface categories.

Response: Examples for the logical interface categories were changed accordingly.

Comments and Responses Regarding Chapter Four, Advanced Metering Infrastructure (AMI) Security Requirements

Comment: Twenty-five (25) commenters suggested that requirements be clear, non-prescriptive, cost effective and scalable based on the criticality of the device or system. Certain requirements also require further clarification and detail.

Response: The second draft of the NISTIR includes requirements for the entire Smart Grid. The security requirements in the second draft of the NISTIR are at a high level and do not specify specific solutions or controls. The AMI requirements included in the first draft of the NISTIR were developed by the Advanced Security Acceleration Project for the Smart Grid (ASAP–SG) project as part of the AMI Security Profile document which is now being maintained by the UCA International Users Group (UCAIug) Smart Grid (SG) Security working group.

Comment: One (1) commenter suggested removing "AMI" from the section title and adding a section on "Smart Grid Control Systems Security Requirements" to this section.

Response: The chapter was revised to address security requirements for the entire Smart Grid and the title of the chapter was changed to "High-Level Security Requirements."

Comment: One (1) commenter recommended that the requirements be refined to remove statements requiring "all components" to include security features. Many security requirements can effectively be handled in a central "system" method.

Response: The second draft of the NISTIR includes security requirements for the entire Smart Grid. The security requirements in the second draft of the NISTIR are at a high level and do not specify specific solutions or controls.

Comment: One (1) commenter proposed that the requirements should be more flexible to allow alternatives that meet the security requirement for efficiency and effectiveness.

Response: The second draft of the NISTIR includes requirements for the entire Smart Grid. The security requirements in the second draft of the NISTIR are at a high level and do not specify specific solutions or controls.

Comment: One (1) commenter suggested that the AMI-Security Task Force (SEC) requirements should be included in an informative annex and not in the main body of the document.

Response: The second draft of the NISTIR includes requirements for the entire Smart Grid, not just on AMI. The AMI requirements will be included in a reference list that will be added to the final version of the NISTIR.

Comment: One (1) commenter proposed that the focus should be on how to secure the transported information through the Internet rather than discourage its use.

Response: The second draft of the NISTIR includes requirements for the entire Smart Grid. The security requirements in the second draft of the NISTIR are at a high level and do not specify specific solutions or controls. Use of the Internet is a specific solution.

Comment: Thirteen (13) commenters provided comments about specific AMI controls. Suggestions included:

- Text revisions for technical content.

• Inquiries regarding clarification or further detail.
• Deletion of text.
• Accidental omissions.
• Concerns regarding specific use cases.
• Inconsistency in terminology.
• Inclusion of additional relevant controls.

Response: The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP–SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. The eighty-six (86) comments were forwarded to the ASAP–SG team.

Comment: One (1) commenter recommended that there are two further pieces of work that will be vital to the success of this project, and in which the security research community could be engaged, as they are of technical interest as well as being important.

1. Security policy for the core of the network.

2. Information flow policies at the periphery (between the meter, home and network).

Response: An R&D sub-group was established under the SGIP CSWG and a chapter in the second draft of the NISTIR includes R&D themes. This comment has been forwarded to that group for evaluation and potential inclusion in the final version of the NISTIR.

Comments and Responses Regarding Appendices

Comment: Five (5) commenters suggested additional use cases to include in the document or edits to existing use cases.

• Additions to Retail Power Electricity Market Use Case.
• Considerations for variation in:
  ○ Real Time Pricing (RTP) for Customer Load and Distributed Energy Resources (DER)/Plug-in Electric Vehicles (PEV).
  ○ Time of Use (TOU) Pricing.
  ○ Power Bulk Electricity Market.

Regional Transmission Operators (RTO).

Independent System Operators (ISO).

Response: The security-relevant content of these use cases will be considered for the final version of the NISTIR.

Comment: One (1) commenter urged NIST to follow a two-track approach in order to address any confidentiality issues: (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.

Response: A strong focus has been placed on reliability, since it is a first priority to the power grid. However, confidentiality is also very critical and the SGIP–CSWG will coordinate with State and Federal policy makers when developing future versions of the NISTIR. The NISTIR focuses on high level security requirements and not specific controls that are implementation specific. Outreach to Federal and State representatives and private sector organizations are an important task and will be considered for the future.

Comment: Thirteen (13) commenters recommended changes and updates to use cases presented in Appendix A. Examples of such recommendations include:

• Revisions to the retail power electricity market scenario.
• Revisions to reflect continuing regional diversity in wholesale power markets.
• Refine statements regarding power system operations to demonstrate some portions of a power system can cease operations without an objectionable impact on the overall power system.
• Clarification that the Use Cases are not mandatory.
• Design considerations to assist people with the use/application of the document.
• Concerns regarding impact (financially to the Utility and to customer trust) of incorrect data.

Response: The Use Cases presented in Appendix A are neither exhaustive nor complete. New Use Cases may be added as they evolve in future versions of this document. The Use Cases were derived "as-is" from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns. The section introduction has been modified to reflect this more clearly.

Comment: One (1) commenter suggested it would be helpful to have a tool to help resolve conflicts between relevant standards. It is not clear which document should be followed for each security requirement in the Draft NISTIR.

Response: Appendix B has been revised to only list the source documents and not standards, that were used in developing the security requirements in the NISTIR. The final version of the NISTIR will list the specific requirements; therefore, individuals will not need to refer to the source documents.

Comment: One (1) commenter was concerned that statements in Appendix D.4, *Openness and Accessibility of Smart Grid Standards,* could be misconstrued to imply that simply because there is a charge for a standard that the standard is not "accessible." Neither openness nor accessibility demands that documents be made available without charge.

Response: The language was changed to avoid possible confusion in associating these standards with closed, secretly developed algorithms.

Comment: Ten (10) commenters provided additional references for inclusion in the NISTIR or changes to existing references.

Response: These references will be considered in developing the final version of the NISTIR.

Comment: One (1) commenter suggested additional information regarding cryptography and key management.

Response: Cryptography and key management are important areas for the Smart Grid. They will be examined more fully in the final version of the NISTIR and a new sub-group has been established to address these topics.

Request for Comments: NIST seeks public comments on the second draft of NISTIR 7628. The report will be revised on the basis of comments received and a final version is scheduled to be posted in late spring of 2010.

The document will contain the final set of security controls and the final security architecture.

Comments on draft NISTIR 7628, *Smart Grid Cyber Security Strategy and Requirements,* may be transmitted electronically to: *csctgdraftcomments@nist.gov.* They also may be mailed to: Annabelle Lee, National Institute of Standards and Technology, 100 Bureau Dr., Stop 8930, Gaithersburg, MD 20899–8930.

Comments must be received no later than June 2, 2010.

E.O. 12866: This notice has been determined not to be significant for the purposes of E.O. 12866.

Dated: April 7, 2010.

Marc G. Stanley,

Acting Deputy Director, NIST.

[FR Doc. 2010–8415 Filed 4–12–10; 8:45 am]

BILLING CODE 3510–13–P