UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-

October 6, 2010

The Honorable Jon Wellinghoff
Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Dear Chairman Wellinghoff:

The Smart Grid team at the National Institute of Standards and Technology (NIST) has been working closely with Federal Energy Regulatory Commission staff to coordinate our efforts and ensure that each of our organizations can accomplish their respective responsibilities under the 2007 Energy Independence and Security Act (EISA).

Through this letter, I am advising the Commission that NIST has identified five foundational families of standards as ready for consideration by regulators. These standards are fundamental to Smart Grid interoperability overall and, specifically, to several FERC priority areas as identified in the Commission's July 16, 2009 Smart Grid Policy Statement. As described in greater detail in the enclosure, these consensus standards, developed by the International Electrotechnical Commission (IEC), help to enable efficient and secure exchanges of information within and across Smart Grid domains.

- IEC 61970 and IEC 61968: Provide a Common Information Model (CIM) necessary for exchanges of data between devices and networks, primarily in the transmission (IEC 61970) and distribution (IEC 61968) domains.
- IEC 61850: Facilitates substation automation and communication as well as interoperability through a common data format.
- IEC 60870-6: Facilitates exchanges of information between control centers.
- IEC 62351: Addresses the cyber security of the communication protocols defined by the preceding IEC standards.

These standards are identified because they are essential to uniform and interoperable communication systems throughout the grid and will accommodate the evolution of the grid and the integration of new technologies. They focus on the information models and protocols important to efficient and reliable grid operations.

NIST has developed a collaborative process that engages Smart Grid stakeholders in identifying prospective interoperability standards and evaluating these specifications against selected criteria, which include considerations such as stakeholder consensus, domains of applicability, and especially cyber security. All of the standards identified in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* support interoperability of Smart Grid devices and systems. As noted in that document, many of the standards are still undergoing development and require modifications, some of which are being addressed through Priority Action Plans (PAPs) being carried out within NIST's Smart Grid Interoperability Panel (SGIP). In reviewing whether a standard is ready for consideration by regulators, NIST

considered a number of factors, including maturity of the standard, whether issues being addressed through SGIP PAPs have been resolved, the existence of technical narrative summary documents describing its application to the Smart Grid, and a review of cyber security requirements. This is the first set of standards that NIST has identified as ready for consideration by regulators. The Smart Grid domains and functionalities of the standards identified by NIST as ready for consideration by regulators are described in the technical narrative summaries; these standards also have undergone cyber security reviews. We anticipate that this process will yield continuing benefit to regulators and other Smart Grid stakeholders as we together work vigorously to achieve the objectives of EISA.

As always, we are interested in feedback to identify opportunities for improving the usefulness of our efforts and our outputs.

Sincerely,

George Arnold
National Coordinator for Smart Grid Interoperability

Enclosure

cc: Jason Bordoff
Commissioner Garry Brown
Commissioner Paul A. Centolella
Aneesh Chopra
Commissioner Tony Clark
Commissioner David C. Coen
Commissioner Lib Fleming
Patrick Gallagher
Commissioner Maureen Harris
Patricia Hoffman
Commissioner Orjiakor N. Isiogu
Commissioner Cheryl A. LaFleur
Commissioner Philip D. Moeller
Commissioner John R. Norris
James Pederson
Commissioner Phyllis Reha
Jamie Simler
Commissioner Marc Spitzer
Philip Weiser

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-

# NIST-identified Standards for Consideration by Regulators
## Release 1.0
## October 6, 2010

NIST has identified five families of foundational standards as ready for consideration by regulators. Developed by the International Electrotechnical Commission (IEC), these identified consensus standards are:

- IEC 61970 and IEC 61968: Provide a Common Information Model (CIM) necessary for exchanges of data between devices and networks, primarily in the transmission (IEC 61970) and distribution (IEC 61968) domains.

- IEC 61850: Facilitates substation automation and communication as well as interoperability through a common data format.

- IEC 60870-6: Facilitates exchanges of information between control centers.

- IEC 62351: Addresses the cyber security of the communication protocols defined by the preceding IEC standards.

These standards are essential to uniform and interoperable communication systems throughout the Smart Grid, and they will accommodate the evolution of the grid and the integration of new technologies. In particular, the standards specify object models that are the basis for efficient exchanges of information between applications within and among grid domains – beginning, primarily, with generation, transmission, and distribution. Broad implementation of these standards will enhance the interoperability of applications and reduce the time and expense required to integrate new technologies and systems.

These standards will further efforts to achieve efficient and secure intersystem communications as well as support other Federal Energy Regulatory Commission (FERC or Commission) priorities identified by the Commission in its Smart Grid Policy Statement, issued on July 16, 2009. These standards are extensible and will be updated as Smart Grid requirements evolve.

To illustrate this dynamic situation and the associated needs for extensibility and harmonization of standards, NIST notes that several Priority Action Plans (PAPs) are being carried out under the auspices of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by NIST with American Recovery and Reinvestment Act funding from the Department of Energy, to address the need to ensure that the standards identified here will accommodate and facilitate interoperability with the grid's legacy systems. The five families of IEC standards identified here by NIST as ready for consideration by regulators are supported by standing IEC technical committees and working groups, and users groups who have adopted the standards are developing methods and means to ensure interoperability. Additionally, the IEC CIM provides an important foundation for extensions of Smart Grid communications into the customer domain.

NIST

## Background

All of the standards identified in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*[1] support interoperability of Smart Grid devices and systems. Through a transparent and highly participatory public process, NIST identified 25 Smart Grid-relevant standards as "ready for implementation" and an additional 50 standards warranting "further review." The two sets of standards and the "guiding principles for identifying standards" were presented in Chapter 4 of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*. As noted in this document, many of the standards are still undergoing development and require modifications, some of which are being addressed through SGIP PAPs. In reviewing whether a standard is ready for consideration by regulators, NIST considered a number of factors, including maturity of the standard, whether issues being addressed through the PAPs have been resolved, the existence of technical summary documents describing its application to the Smart Grid and a review of cyber security requirements.

With respect to cyber security, *all* existing and new standards identified as supporting Smart Grid interoperability must undergo a thorough cyber security review. This essential task could not be accomplished until the SGIP Cyber Security Working Group (CSWG) had completed its *Guidelines for Smart Grid Cyber Security,* which NIST issued on September 2, 2010.[2] These guidelines include nearly 200 high-level security requirements and identify an initial set of 137 Smart Grid interfaces. The CSWG review of the first five standards put forth for regulatory consideration can be found on the CSWG website.[3]

All of the other standards identified in Release 1.0 as well as those identified in future NIST and SGIP activities will undergo cyber security reviews. Results of these reviews will be made publically available on the CSWG website.[4] Standards organizations and prospective users of the reviewed specifications can use this information to address identified gaps or other issues.

## First Set of Standards Ready for Consideration by Regulators

With input from collaborators including the SGIP administrator, relevant working group chairs and members of the Standards Developing Organizations (SDOs), regulators and others, NIST has developed technical narrative summaries of the technical contents of Smart Grid standards identified through the NIST process, including their applications, potential issues, and the results of the cyber security review.

NIST has posted technical narrative summaries for five families of standards to assist FERC, state and local regulators, and other interested Smart Grid stakeholders.[5] These five IEC standards are concerned with the structure of messages exchanged within and across Smart Grid domains and are fundamental to interoperability.

---

[1] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (Special Publication 1108),* Jan. 2010. Available at: http://nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.
[2] The three volumes of *Guidelines for Smart Grid Cyber Security (NISTIR 7628)* can be downloaded at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
[3] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards/StandardsReviewPhase-1Report.pdf
[4] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards
[5] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTStandardsSummaries

- IEC 61970, Energy Management System Application Program Interfaces (EMS-API), and IEC 61968, Application Integration at Electric Utilities: These families of standards define information exchanged among control center systems using a Common Information Model (CIM). They define application-level energy-management-system interfaces and messaging for distribution grid management.

- IEC 61850, Communications Networks and Systems for Power Utility Automation[6], Parts 1-6, 7-1 to 7-4, 8-10, and 90: Defines communications within transmission and distribution substations for automation and protection. It is being extended to cover communications beyond the substation to integration of distributed resources and communication between substations.

- IEC 60870-6-503: TASE.2 Services and Protocol; IEC 60870-6-702: Functional Profile for Providing the TASE.2 Application Service in End Systems; IEC 60870-6-802: TASE.2 Object Models; and IEC TR 60870-6-505 Amendment 1: TASE.2 User Guide: These Telecontrol Application Service Element (TASE.2) standards facilitate control center (telecontrol) data exchange, and they may be applied in any other domain with comparable requirements, including power plants. The standards define the electric power system status and control messages sent between control centers of different utilities.

- IEC 62351: Power Systems Management and Associated Information Exchange – Data and Communications Security: These standards cover information security for power system control operations. They specify security requirements for communication protocols defined by IEC Technical Committee 57, specifically the IEC 60870-5, the IEC 60870-6, the IEC 61850, the IEC 61970, and the IEC 61968 families.

**Other Considerations**

Cyber security requirements were often not included in power grid communication standards in the past and as a result, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented." With the advent of the Smart Grid, cyber security has become increasingly important, but since the development cycles of communication standards and cyber security standards are usually independent of each other, appropriate normative (mandatory) references between these two types of standards are often missing. Over time, these missing normative references will be added. With the rapid improvement of technologies, obsolescence of older technologies may occur, but may be mitigated by specifying minimum requirements and promoting greater compliance to new technologies as they are developed and verified. The CSWG Standards Review (Review)[4] recognizes the need to improve the inclusion of normative references in the five standards identified here, as well as the lag between the development of the latest cyber security technologies and their inclusion in the standards by making recommendations for improvement of the standards. The Review includes two recommendations: 1) that at their next revision the IEC CIM and communication standards should include normative references to the IEC 62351 family of security standards, and 2) that

[4] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards

the IEC 62351 standard should be updated to address the latest security enhancements and new technologies as part of their next revision cycle.

The nation's electric power grid spans geographic and jurisdictional boundaries and economic sectors. Depending on their relevance to particular functions and domains, consensus standards identified by NIST as applicable to achieving an interoperable Smart Grid will be of interest to FERC, state and local regulators, and other stakeholders. Future installments of NIST-identified standards will be germane to multiple stakeholders, including commercial and residential consumers.

The diversity of Smart Grid stakeholder groups is represented on the SGIP, which NIST launched in November 2009 and now has more than 600 organizational members. NIST is confident that the SGIP will be an important asset in the sustained effort required to build the standards infrastructure for a modernized power grid. All the activities and resulting outputs of NIST's standards-related efforts have been made available to the public, and all major documents have been accessible for public review and comment. This introduces additional steps into the process, but the quality of the comments received has been worth the investment of extra time and effort, and provides additional assurance of consensus on the interoperability standards that emerge. NIST will continue to make available its outputs to all interested organizations or individuals, and will continue to coordinate with federal and state regulators in its ongoing efforts to achieve the objectives of the Energy Independence and Security Act of 2007.