UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Smart Grid Policy) Docket No. PL09-4-000

COMMENTS OF THE
CALIFORNIA INDEPENDENT SYSTEM OPERATOR CORPORATION
ON THE COMMISSION'S PROPOSED POLICY STATEMENT AND ACTION PLAN

The California Independent System Operator Corporation ("ISO") respectfully submits these comments in response to the Commission's Proposed Policy Statement and Action Plan on Smart Grid policy ("Policy Statement"). The ISO welcomes this opportunity to share its views on the Policy Statement.

I. BACKGROUND

On March 19, 2009, the Commission issued the Policy Statement in a newly-opened docket on smart grid policy. The proceeding has two purposes. The first purpose is to develop interoperability standards in six smart grid areas. The Energy Independence and Security Act of 2007 ("EISA") mandates that the National Institute of Standards and Technology ("NIST") coordinate the development of standards and protocols on smart grid functionalities with industry standards groups. EISA also orders FERC to adopt those standards once NIST has developed sufficient consensus on the standards it helps coordinate. The Policy Statement is a preliminary step in that process.

The second purpose of the Policy Statement is to set an interim rate policy to cover smart grid expenditures made before FERC develops a complete smart grid policy. Pending adoption of definitive smart grid rate recovery standards, the

Commission proposes to allow cost recovery of smart grid expenditures made in the interim provided that the applicant can demonstrate that: (1) the project will not adversely impact reliability; (2) the likelihood of creating stranded costs is minimized; and (3) it will share information about the project with the U.S. Department of Energy's Smart Grid Clearinghouse.

The Policy Statement sets out FERC's proposed approaches in these areas and seeks comment on the proposals.

II. GENERAL COMMENTS

Before addressing the specific issues raised in the Policy Statement, the ISO first wishes to address a few general topics. The ISO first notes that it limits its comments to the issue of interoperability standards. The ISO takes no position on the Commission's proposed interim rate recovery policy.

A topic of significant importance is the Commission's and NIST's approach to setting standards. As the ISO understands EISA, NIST's role is not to adopt standards on its own. Rather, its role is twofold. The first role is to identify existing standards that the Commission should consider adopting formally. The second role is to identify gaps in the current standards process and engage with appropriate standards development organizations to fill those gaps. The ISO believes that this is a prudent approach and strongly encourages NIST and the Commission to follow it. At present, there is no shortage of work on technical interoperability standards. This work is currently being conducted by industry groups that have the necessary technical knowledge. If anything, at this point there is the risk of creating too many, possibly conflicting, standards. For this reason, NIST and the Commission should focus on coordinating these ongoing processes and setting priorities.

The ISO also notes that there is a great deal of overlap among the six topics in the Policy Statement that are related to standards development. For this reason, standards pertaining to one topic should be developed with an awareness of the need for standards on other topics. As a preliminary example, cyber-security standards developed in isolation may include high levels of data encryption that may be too cumbersome to allow for the rapid transfer of data necessary for smart grid applications. It is for this reason that it is important that NIST and FERC effectively coordinate the various existing standards and make sure they are harmonized. Thus, NIST and FERC should not be active in creating standards themselves. They should, however, be very active in making sure that outside parties develop standards in a way that pays attention to the many inter-related, and sometimes conflicting, aspects of the smart grid. One of the ISO's goals in this filing is to highlight some of the many ways that these various topics relate to each other.

One final preliminary comment is that the ISO would like to highlight the role wholesale market design can play in facilitating development of a smart grid. The ISO went live with a major market redesign on April 1, 2009. Part of this redesign will create greater transparency and understanding in terms of where there is congestion on the system and where resources should be dispatched. Gaining a better understanding over this type of issue will help enable integration of intermittent renewable resources and energy storage, which are both part of the smart grid concept. A wholesale energy and transmission market that allows a more refined and granular understanding of what is happening on the grid is thus the skeleton onto which smart grid functionalities can be built. While the ISO would not necessarily advocate that the Commission adopt a single generally applicable market design, the Commission can use its oversight of wholesale electricity markets to guide their development in a direction that will embrace current and future smart grid technologies.

III. CYBER-SECURITY AND RELIABILITY

The issue of cyber-security presents an irony. One of the goals of smart grid is to improve reliability by creating greater visibility over the electric grid and helping grid operators localize outage disruptions and prevent cascading failures. This visibility occurs by linking together more parts of the transmission and distribution system and increasing the flow of communication on the system. However, some parts of the system have weaker security standards than others. By creating more linkages, system security can become weaker, as the strength of an interconnected system is determined by its weakest part. Thus, in the process of reducing the likelihood of outages due to human error and weather-related events, a smart grid simultaneously can increase the risk of outages from ill-intentioned actions if security is not considered across the entire network. Without proper regard for cyber-security, the smart grid poses the danger of creating a one step forward, two steps back circumstance with regard to system reliability. It is for this reason that the ISO applauds the Commission for making cyber-security and reliability standards a priority in setting smart grid standards.

The ISO's major security concern with a smart grid is that the grid may face vulnerabilities that fall beyond the ISO's currently established electronic security perimeter. Under NERC's security and reliability regulations, the ISO currently is responsible for the security of its own internal systems. The ISO additionally creates secure communications links with market participants through its External Entity Access Requirements and Agreements. The smart grid involves technologies such as Advanced Metering Infrastructure and Home Area Networks, both of which gather information at the customer's location and feed that information to the local utility, which in turn provides that aggregated information to transmission operators like the ISO. Such equipment vastly increases the number of portals that ultimately feed information into the ISO's system. While there will not be a direct link from, *e.g.*, a smart meter into the ISO's system, smart meters provide information that may be transmitted into the ISO's system. Such information will provide the basis for generator dispatch and other grid operations decisions. If the security of such data were compromised, it ultimately could lead to problems on the ISO's system. The problem is that responsibility for such security lies in the hands of parties beyond the ISO's control. By the time corrupted data is fed to the ISO it has been aggregated and there is little way for the ISO to be aware that the data it is relying upon to operate the grid has been compromised. This is already a potential problem. However, a smart grid makes it a greater concern by increasing the points of entry into utilities' systems. Thus, a smart grid has the potential for making ISOs and Regional Transmission Organizations ("RTOs") responsible for maintaining the security of systems that are beyond their control.

Another difficult issue posed by a smart grid is that requiring a robust demonstration from project proponents that their projects will not jeopardize security can itself create security risks. In theory it makes sense that smart grid projects should be required to demonstrate that they will not jeopardize security. However, imposing such a requirement presents practical problems. System security is a matter of creating multiple layers of security. A security feature of one piece of equipment cannot be understood without understanding the context of the entire web of interlocking layers of security. Providing that context raises the possibility that outside parties could identify and exploit any potential gaps in security.

The Commission proposes a two-pronged approach to address the many security issues, such as the ones discussed above, raised by the smart grid. The first is that entities subject to Commission-approved standards, such as NERC's Critical Infrastructure Protection ("CIP") standards, must maintain compliance with those standards. The second is that smart grid technologies must address the following five factors: (1) how data will be protected; (2) how communications between grid components will be authenticated; (3) how the applicant will prevent unauthorized modifications of smart grid devices; (4) how the smart grid devices will be physically protected; and (5) how the unauthorized use of a smart grid device could impact the bulk-power system.

The ISO believes that the first prong of this approach is sufficient. NERC's current CIP standards already would seem to address these five issues. To the extent they are not addressed by CIP standards, the better approach would be for NIST to engage NERC to revise the CIP standards and expand them to deal with the security issues posed by the smart grid. In this case, it makes little sense for NIST to coordinate the adoption of completely new standards. NERC's standards already are binding because of its role as the nation's Electric Reliability Organization. Thus any new standards should be tailored carefully to ensure that they do not conflict with NERC's existing standards. NERC has the greatest expertise in understanding how any new standards would interact with the current standards. NERC also has experience in conducting confidential audits of utilities. Applying NERC's current confidentiality rules could address the problem of increasing the risks to security by forcing project proponents to demonstrate their adherence to security standards. Relying on NERC has the added benefit of making it easy for ISOs to continue their involvement in setting security and reliability standards. ISOs and RTOs have been active in working with NERC at developing and refining CIP standards. By keeping NERC's leadership role in security and reliability, the Commission will also make it easier for ISOs and RTOs to continue contributing to NERC's important work.

IV. INTER-SYSTEM COMMUNICATION AND COORDINATION

The ISO largely agrees with the Commission's proposed approach to developing standards for inter-system communication and coordination. The ISO also observes that the issue of inter-system communication is a perfect example of the interrelationships of various smart grid functionalities. As discussed above, the smart grid creates new security vulnerabilities precisely because so many different systems will communicate with each other. Thus, inter-system communication standards cannot be developed without due regard for cyber-security. As will be discussed below, effective inter-system communication will be a prerequisite for creating what the ISO calls "deep-area situational awareness." Similarly, effective inter-system communication will be essential for demand response. Without a reliable way for ISOs and RTOs to be informed of consumers' responses to changing system dynamics, grid operators cannot adjust generation dispatch accordingly.

V. WIDE-AREA SITUATIONAL AWARENESS

A. The Usefulness of Phasor Measurement Units

The ISO concurs with FERC's identification of the role phasor measurement units ("PMUs") will play in creating wide-area situational awareness. At present, though, there are limits to their usefulness. One major limit on their usefulness is the robustness of the communications infrastructure. Without high-quality communications infrastructure, information will not be delivered to ISOs and RTOs in time for it to be useful. The speed with which that data is communicated among the different system elements will also depend on the level at which the data is encrypted. These two limiting factors again highlight the fact that standards in one area of the smart grid cannot be developed in isolation.

The Policy Statement highlights the efficiency aspects of PMUs because they conceivably will allow for dynamic line rating. Thus far, however, PMUs' greatest use has been for reliability and incident reconstruction. The efficiency benefits from things like dynamic line rating require additional research. An example is dynamic dampening control. The California Oregon Intertie ("COI"), a set of high-voltage lines linking the Pacific Northwest with California and other states in the Southwest, has an operational limit of 4,800 MW, but a thermal rating substantially above that. The lower operational limit is due to frequency and voltage oscillations. With wider deployment of PMUs, the system operator could know how and when to use electric storage to send a momentary pulse of electricity to dampen the oscillation and increase the amount of energy transmitted over the lines. However, without well-developed energy storage devices, there is limited ability to quickly send such a pulse. Again, the effectiveness of one area of smart grid (wide-area visibility) is affected by another area (electric storage). Standards on the deployment of PMUs should be developed with the above-mentioned factors in mind.

Part of developing technical standards for PMUs should include a coordinated and thoughtful approach to where new PMUs should be located. Most PMUs have been placed near electric generating stations because generation stations are the main cause of frequency oscillations. However, such oscillations can also be caused by the power that is fed into the ISO's system at the interties. Placing PMUs at the interties may help refine the state estimator by getting a clear view of interchanges between balancing authority areas. Currently, if there is a problem in a remote location, the ISO must rely largely on person-to-person communications to understand what the problem is and then project forward how it will impact the ISO's system. Widespread deployment of PMUs at the interties would mean that the ISO would no longer have to rely on person-to-person communications. PMUs at the interties would provide balancing authority areas immediate visibility of interchanges. By tying such information into the state estimator, the ISO also would have a better idea of how to react to the new information.

B. The North American SynchroPhasor Initiative

The ISO agrees with the Commission that the North American SynchroPhasor Initiative ("NASPI") will be a key part of creating PMU standards.

The exchange of information fostered by NASPI has led to new communication standards for PMUs. The ISO has been an active part of such efforts. The Policy Statement suggests that ISOs and RTOs take a leadership role in NASPI. It is reasonable to have ISOs and RTOs take a leading role because they will gain the greatest functionality from widespread deployment of PMUs. Individual transmission utilities enjoy limited benefits from their PMUs. It is the aggregated information provided by PMUs system-wide that will create the most significant benefits.

C. Deep-Area Situational Awareness

In the future, the ability to look across wide areas will only tell a transmission operator part of the story. As distributed generation, storage, and controllable loads are deployed as part of a smart grid, most of these resources likely will be interconnected at the distribution, rather than the transmission, level. The result will be that the centrally dispatchable resources that an ISO or RTO uses to schedule and balance the bulk-power system will constitute a decreased share of the total resources on the grid, while resources within the distribution grid (which currently are invisible to a system operator) will constitute an increased share of the total grid resources. Without making at least some of these new distribution-level resources explicitly visible to an ISO or RTO, the efficient and reliable operation of the smart grid could be jeopardized.

It is in this context that the ISO introduces its concept of "Deep-Area Situational Awareness." Successful operation of the smart grid will require a broader and a deeper understanding of the operational state and capabilities of resources, both across the transmission grid as well as into the distribution grid. It is with this in mind that the ISO urges that particular attention be paid to the identification and/or development of inter-system communication standards that address the transmission/distribution interface. The standards already identified by the Commission can be of potential benefit. For example, IEC 61970 (CIM) can facilitate a shared model of the distribution and transmission assets. It is also important to assess the efforts of the Cigré Working Group D2.24 to extend the concepts of IEC 61968 from its original focus on distribution utilities to address the needs of transmission operators. Additionally, the expansion of IEC 61850 from its role in distribution substations to an end-to-end communications system suggests a path forward.

Finally, it is important for distribution-level utilities to gain wide-area visibility over their own systems so that they can operate their systems more efficiently. The ultimate goal in this regard is to have wide-area awareness on *both* the distribution and transmission system simultaneously *plus* effective flow of that information between the operators of the distribution and transmission systems. Any standards should be developed with this end goal.

VI. DEMAND RESPONSE

The ISO supports the Commission's observation that establishing interoperability standards between devices and systems and communication protocols between the parties and systems engaged in a demand response transaction is vitally important and worth FERC's immediate attention. Moving forward, adopting standards can be an important role for the Commission and much can be gained from the Commission's leadership in this area.

The Commission proposes to utilize "use cases" to create standardization around demand response to help address challenges on the bulk-power system. An emphasis of such use cases would be to develop particular scenarios that focus on increasing demand during over-generation conditions and responding to the unavailability of intermittent resources. The ISO supports the use case approach as an important step in defining the requirements necessary for demand response resources to make the bulk-power system more reliable and to support the integration of additional intermittent renewable resources. As a first step, FERC should consider leveraging the plethora of available demand response use cases and then evaluate the need for additional use case development, where appropriate.

The Commission also seeks comment on whether the Open Automated Demand Response ("OpenADR") standard merits close consideration. The Commission should encourage open standards and inter-operability. Closed architecture and proprietary communication protocols can make application development difficult and cost-prohibitive. The ISO believes that the OpenADR standard is timely and appropriate. The UCA International User's Group and the Organization for the Advancement of Structured Information Standards are currently standardizing OpenADR. As such, once the standardization work is complete, the Commission should consider adopting OpenADR because OpenADR can spur innovation and new investment in demand response.

In setting any standards in demand response, it is important to keep in mind that demand response will be a product of two factors: inter-system communication and appropriate market signals sent through tariffs. Once reliable communications systems are in place, the success of demand response likely will be more a matter of creating proper incentives for load to respond to market dynamics than of setting proper technical standards. Creating such incentives is largely beyond the Commission's control, as such matters are more within the jurisdiction of state utility commissions. Thus, the Commission's adoption of appropriate technical standards for demand response should be seen as a necessary, but not sufficient, step towards meaningful demand response.

VII. ELECTRIC STORAGE AND TRANSPORTATION

The standards-setting issues with electric storage and plug-in hybrid electric vehicles ("PHEVs") are largely the same. These technologies are in their incipiency. The Commission suggests that setting standards early will encourage additional investment and facilitate further development. If that is the goal, then standards should be set in light of that goal. Accordingly, detailed technological standards are not what are needed at this early juncture. The standards that are needed should address basic structural, competitive, and architectural issues. For example, with PHEVs, one basic structural question is whether the meter that measures the vehicles electric consumption should be located in the vehicle or at the location where the vehicle is charged. Keeping the meter in the vehicle enhances mobility by making it easier to charge the vehicle in multiple locations. But keeping the meter tied to a physical location, such as the vehicle owner's home, allows a utility to keep better track of the vehicle's usage and likely will better enable PHEVs to serve as storage devices.

The ISO believes that the problem of incorporating both PHEVs and electric storage into the electrical system largely will be solved through tariffs, not technology. For example, the ISO has been working to redefine ancillary services in terms of its ability to provide certain functionalities. The ISO is looking to make its definition of ancillary services technology-neutral and not tied specifically to generation. By doing so, there will be a clearer path for storage, as well as other emerging and yet-to-be invented technologies, to become a meaningful part of the system the ISO operates. Similarly, in the Policy Statement, the Commission raises the issue of how to deal with the potential problem of PHEVs being charged during peak times, and thus increasing peak load, rather than charging at off-peak times, and thus smoothing the load profile. Again, the ISO does not believe this is a technological problem. Instead, tariffs that provide proper incentives for charging at off-peak times will address this problem most directly.

VIII. CONCLUSION

The ISO welcomes this opportunity to provide feedback to the Commission on its Proposed Policy Statement and Action Plan on Smart Grid Policy. Facilitating the development of the smart grid is an important policy objective. The ISO intends to take an active role in this proceeding in order to assist the Commission in carrying out this vital role.

Dated: May 11, 2009 Respectfully submitted,

/s/David S. Zlotlow
Nancy J. Saracino
Vice-President, General Counsel Corporate Secretary
Anthony J. Ivancovich
Assistant General Counsel –Regulatory
David S. Zlotlow
Counsel
California Independent System Operator Corporation
151 Blue Ravine Road
Folsom, CA 95630
Tel: (916) 608-7007
Fax: (916) 608-7296

Counsel for The California Independent System Operator Corporation

CERTIFICATE OF SERVICE

I hereby certify that I have served the foregoing document upon the entities that are described in that document as receiving service, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Folsom, California this 11th day of May, 2009.

/a/ Jane Ostapovich
Jane Ostapovich