Item 43
(10738)

State of California **Public Utilities Commission**
San Francisco

M E M O R A N D U M

Date : October 14, 2011

To : The Commission
(Meeting of October 20, 2010)

From : Wendy Al-Mukdad, Energy Division
Chris Villarreal, Policy Planning Division
Elizabeth Dorman, Legal Division

Subject : Staff Seeks Authority To File Comments On The U.S. Department of Energy *Electricity Sector Cybersecurity Risk Management Process Guideline* Proposal

I. EXECUTIVE SUMMARY

The Staff of the California Public Utilities Commission (CPUC or Commission) seeks permission to file comments on behalf of the Commission with the U.S. Department of Energy (DOE) regarding its proposed *Electricity Sector Cybersecurity Risk Management Process Guideline* (Guideline). CPUC Staff believes this proposal may be developed into a useful tool for the CPUC and jurisdictional Load Serving Entities in their efforts to modernize California's electrical transmission and distribution system to maintain safe, reliable, efficient and secure electrical service using cost-effective digital information and control technology consistent with Senate Bill 17.[1] Such technical infrastructure developments are commonly referred to as the smart grid.[2]

[1] Senate Bill 17 requires the CPUC to evaluate various potential capabilities of the smart grid including customer enablement, energy efficiency, demand response, renewable resource integration and other technologies that may facilitate California's goals for reducing greenhouse gasses. It also requires CPUC to report to the Governor and Legislature annually on the CPUC's recommendations and status of deployment of various smart grid technologies by Load Serving Entities, as well as the costs and benefits to ratepayers of such developments. Cal. Pub. Utils. Code § 8360 and subd. (a), available at http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_17_bill_20091011_chaptered.html (SB 17).

[2] Id.

Staff requests authority to submit comments generally supporting use of the Guideline as a basis from which to develop a final product. Specific suggestions that Staff believes may strengthen the Guideline include:

1) The Tiers Structure could be improved by clarifying the definitions and functions of each Tier, particularly how they align with existing and anticipated organizational structure.
2) The Guideline may be strengthened by being more narrowly tailored to challenges posed to smart grid deployment for electric utilities.
3) The Guideline may be more effective if it includes more practical implementation recommendations, particularly for incorporation of risk management activities into smart grid deployment planning.
4) The CPUC Staff recommends that the DOE consider proposing metrics to track effectiveness of risk assessment activities.

II. BACKGROUND

The *Electricity Sector Cybersecurity Risk Management Process Guideline* (Guideline) was developed by the DOE, in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC).[3] The primary goal of the Guideline is to create a risk management process that could be used by electric sector organizations, such as Load Serving Entities, to prevent purposeful or inadvertent damage to electric grid reliability arising from increased reliance upon advanced, integrated information technologies as is contemplated in various initiatives to develop the smart grid. The Guideline is explicitly intended *not* to

> "replace or subsume other risk-related activities, programs, processes or approaches that Electricity Sector organizations have implemented [pursuant to] legislation, regulation, policies, programmatic initiatives, or mission and business requirements. This guidance is not part of any regulatory framework[;]"[4]

but, rather, is intended to be complementary to more comprehensive risk management programs.[5]

[3] See https://public.commentworks.com/CW_DOE_AWF/.

[4] Guideline at p. iii.

[5] Id.

III. COMMENTS

A. The Guideline is a good basis from which to develop a final risk management process model.

The CPUC Staff recommends that the CPUC support the DOE's effort to develop the Guideline and its use as a basis for risk management model. The CPUC Staff supports the goals behind the draft Guideline and believes that it can be a good high-level guidance document for the electric sector. The CPUC Staff believes that the concept of the Risk Management Process, derived from NIST SP 800-39,[6] may be useful in developing cybersecurity policies for utilities, as it guides organizations to establish an enterprise-wide risk management strategy and a mature governance structure. The CPUC Staff believes that this type of structure may, with further development, be appropriately applicable to a variety of entities involved in the conceptualization, implementation, monitoring and regulation of the smart grid.

The Guideline provides a detailed list of activities appropriate for a risk assessment processes, and is intended to address only the management of cyber-security related risk derived from or associated with the operation and use of information technology and industrial control systems. The cyber-security risk management process Guideline is complementary to and should be used as part of a more comprehensive risk management program.

The states and FERC have existing guidelines regarding the reliability of current technologies for grid management. These have traditionally included generation, transmission and distribution functions subject to various types of state and/or federal jurisdiction. The potential of the smart grid comprises a sea change in the variety of technologies that will be incorporated into the distribution and transmission grids of the future. While the California Legislature has chosen to delegate to the CPUC the duty to evaluate and report on smart grid development, existing state and federal authorities do not necessarily have the range of technical resources necessary to develop appropriate risk assessment methods from scratch. Thus, it is appropriate for state and federal agencies concerned with short and long term electricity grid reliability to leverage existing and developing industry standards when considering how to modernize the reliability/risk assessment standards and guidelines for grid operation with respect to new types of grid elements.

The CPUC Staff believes that the Guideline may assist the CPUC in analyzing and developing modern grid features that minimize various risks related to smart grid development. Likewise, the CPUC Staff believes that the Guideline may assist the relevant federal agencies in developing processes, standards and models to implement a

[6] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

reliable smart grid with respect to decisions within their respective decision-making authorities.

Tiers Structure could be improved by clarifying the definitions and functions of each Tier, particularly how they align with utility organizational structure. The Guideline proposes a three-tiered structure consisting of the following Tiers:

Tier 1: Organization
Tier 2: Mission and Business Process; and
Tier 3: Information technology (IT) and industrial control systems (ICS)

The intention of the three-tiered structure is to "provide[] a comprehensive view ... on how risk management activities are undertaken across an organization."[7]

The Tiers structure appropriately reflects that risk assessment activities must take place at varying organization levels. It is unclear, however, whether the tiers are intended to represent types of activities, as described in the Risk Management Model section,[8] or levels in the organization. For example, Tier 1 is first introduced as activities that "address risk from an organizational perspective by establishing and implementing governance structures that are consistent with strategic goals and objectives,"[9] but is later discussed as a Tier that represents an executive function.[10] It appears to CPUC Staff that the tiers are loosely intended to denote the following organizational structures:

Tier 1: Executive
Tier 2: Business Unit Management
Tier 3: Technical Resources

While there is validity to grouping risk management activities either by type (as suggested in the Risk Management Model section) or by level in the organization (as suggested by later sections of the document), it may help to clarify which of the two frameworks the Tiers are intended to represent. Once the definition of tiers has been clarified, a revision of alignment of activities to tiers is likely to be appropriate.

In addition, Tier 3 may need some further development, particularly to expand upon how information would flow to the tiers above. The Guideline proposes a process that allows for a top-down and bottoms-up approach to developing a Load Serving Entity's risk

[7] Guideline at p. 4.[8] Guidelines pp.4 - 6

[9] Guidelines p. 5

[10] Guidelines p. 13

management analysis process, but could benefit from providing additional detail on how a bottoms-up approach is used to revise the goals of each Tier.

B. The Guideline may be strengthened by being more narrowly tailored to industry-specific utility operational requirements.

The CPUC Staff recommends that the guidelines include specific electricity sector examples of smart grid-related risks. The Guideline identifies that smart grid solutions are dependent on two broad types of technologies: information systems (IT) and industrial control systems (ICS).[11] While the initial section of the Guideline discusses some of the characteristics of each type of a system, it may be beneficial to expand upon what unique challenges from a risk management perspective IT and ICS systems pose in a smart grid context.

ICS systems in particular have unique challenges in a utility environment, due to both electrical engineering complexity and real-time nature of their operations. The loss of availability can translate to power outages which directly impact reliability. Therefore, Staff recommends that the Guideline document be expanded to more specifically address how utilities can better manage risks associated with systems that directly affect utility operations.

The Guidelines could also be enhanced by discussing components that may fall outside of traditional IT and ICS systems, but may nevertheless have cybersecurity risks. Manufacturers are beginning to incorporate intelligence into traditional system components, as well as devices that may eventually be part of what is traditionally considered industrial control systems or be tied into information technology systems. That intelligence may or may not be activated by a utility but should be addressed by a cyber-security risk management process.

C. The Guideline may be more effective if it includes more practical implementation recommendations, particularly for incorporation of risk management activities into smart grid deployment planning.

As discussed above, the CPUC Staff recommends that the Commission support the Guideline's goal of developing a risk management process. The CPUC Staff believes, however, that the Guideline could be enhanced by providing a discussion of how to implement this structure in a utility environment. While the draft Guideline provides solid guidance for managing risks associated with existing systems, the CPUC Staff

[11] Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, which in an electricity sector environment include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLCs) and remote terminal units (RTUs).

recommends that the document be broadened to also address the changes that are contemplated as parts of the electric industry's "electric grid modernization" or smart grid efforts. There are many risks to grid modernization and subsequent monitoring that could be minimized by adequate systems engineering and design and the use of cyber-security standards or requirements when planning for infrastructure modernization.

One of the unique aspects of smart grid is the pace of implementation of new technologies and their transformational nature. Not only are new IT and ICS systems being deployed at a rapid rate, in many cases they will change how a utility operates. As such, it would be a useful to get a perspective of how a four-step cyclical approach described in the Guideline could be enhanced to address deployment of systems that introduce new layers of complexity and risks. In particular, the Guidelines could be enhanced by addressing how risk management can be incorporated in project planning and implementation, in addition to ongoing operations.

The CPUC Staff also recommends that the DOE consider proposing metrics to trace the effectiveness of risk assessment activities. The CPUC Staff suggests that specific metrics may provide useful ways to measure the effectiveness of cybersecurity risk management measures, and would propose that the DOE offer an initial set of metrics that can support the various entities in developing effective cyber-security risk management processes and procedures.

IV. ACTION REQUESTED

The CPUC Staff requests that the Commission authorize Staff to submit comments to the DOE and other relevant federal agencies and their delegates[12] consistent with the points discussed above. Comments on the draft Guideline are due to DOE on October 28, 2011.

Please contact Elizabeth Dorman at (415) 703-1415, or at edd@cpuc.ca.gov, if you have any questions or comments.

EDD:cdl

[12] A variety of federal agencies are currently considering, individually and in collaboration, a variety of subjects related to smart grid interoperability, reliability and security; such as the Federal Energy Regulatory Commission (FERC), DOE, NIST. As the CPUC has been involved in a number of these initiatives, it may be helpful to submit comments reflecting these positions in fora beyond the current comments to the DOE.