STATE OF CALIFORNIA ARNOLD SCHWARZENEGGER, *Governor*

PUBLIC UTILITIES COMMISSION
505 VAN NESS AVENUE
SAN FRANCISCO, CA 94102-3298

February 12, 2007

Magalie R. Salas, Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: Mandatory Reliability Standards for Critical Infrastructure Protection
Docket No. RM06-22-000

Dear Ms. Salas:

Enclosed for filing in the above-docketed case, please find an original electronic filing of the attached document entitled **"NOTICE OF INTERVENTION AND COMMENTS OF THE CALIFORNIA PUBLIC UTILITIES COMMISSION**" Thank you for your cooperation in this matter.

Sincerely,

/s/ Laurence G. Chaset

Laurence G. Chaset
Staff Counsel

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Mandatory Reliability Standards
for Critical Infrastructure Protection — Docket No. RM06-22-000

NOTICE OF INTERVENTION AND COMMENTS OF THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

I. INTRODUCTION

On August 28, 2006 the North American Electric Reliability Corporation ("NERC") filed for approval by the Federal Energy Regulatory Commission ("FERC") eight proposed Critical Infrastructure Protection ("CIP") Reliability Standards pursuant to section 215 of the Federal Power Act ("FPA"). NERC'S proposed CIP standards are designed to maintain the integrity of North America's interconnected electrical system by establishing requirements for addressing cyber security, and one standard (CIP-006) addressing physical security.

The CIP standards consist of eight proposed Critical Infrastructure Protection Reliability Standards (CIP-002 through CIP-009). An industry ballot approved the CIP standards on Mach 24, 2006, and the NERC Board of Trustees later approved these standards on May 2, 2006. NERC filed the CIP standards for approval by FERC on August 28, 2006.

On December 11, 2006, FERC released a staff preliminary assessment of the eight proposed CIP Reliability Standards. This assessment is a preliminary technical analysis by staff and does not offer legal conclusions or recommend any particular action to be taken by the Commission. Concurrent with the issuance of this staff preliminary assessment, FERC invited NERC, as well as other interested parties, to respond to this preliminary assessment by February 12, 2007.

II. NOTICE OF INTERVENTION

The California Public Utilities Commission ("CPUC") is a constitutionally established agency charged with the responsibility for regulating electric corporations within the State of California. In addition, the CPUC has a statutory mandate to represent the interest of electric consumers throughout California in proceedings before the FERC.

Communications to the CPUC in this proceeding should be addressed to:

Laurence G. Chaset
Public Utilities Commission of the
State of California
505 Van Ness Avenue, Room 5131
San Francisco, California 94102
(415) 355-5595
e-mail: lau@cpuc.ca.gov

Mark Ziering
Public Utilities Commission of the
State of California
505 Van Ness Avenue, 2nd Floor
San Francisco, California 94102
(415) 703-2233
e-mail: maz@cpuc.ca.gov

Mihai Cosman
Public Utilities Commission of the
State of California
505 Van Ness Avenue, 4th Floor
San Francisco, California 94102
(415) 355-5504
e-mail: mr2@cpuc.ca.gov

Keith D. White
Public Utilities Commission of the
State of California
505 Van Ness Avenue, 4th Floor
San Francisco, California 94102
(415) 355-5473
e-mail: kwh@cpuc.ca.gov

This intervention serves to make the CPUC a party to these proceedings.

III. GENERAL COMMENTS

The CPUC supports the notion of Reliability Standards, including Cyber Security standards. The CPUC supported the UA 1200 – Urgent Action Cyber Security Standards, originally approved in August of 2003, the predecessor to the CIP standards. The CIP standards are Cyber Security standards created by NERC that apply to all appropriate entities and dictate to the entities the measures that should be taken to ensure security. The CPUC generally agrees with the proposed CIP standards, but has two general issues to comment on: firstly, the discretion given to each applicable Entity in using the Business Judgment Rule; and secondly, the applicability of the proposed standards.

A. Discretion in using the Business Judgment Rule

The CPUC shares FERC Staff's concern with the language in each standard, specifically with the discretion given to each entity in applying a Reliability Standard using "reasonable business judgment". The CPUC believes that applying business judgment to a cyber security standard is illogical and incompatible. A certain degree of discretion should be allowed, and a certain measure of flexibility is needed for successful implementation. But reasonable business judgment has no place in implementing cyber security, as highlighted in the following discussion.

The Business Judgment Rule applies to actions of a corporation's board of directors in managing the corporation. It deals with the operations and business decisions. The notions underlying cyber security, on the one hand, and the Business Judgment Rule, on the other, are mutually exclusive. The Business Judgment Rule essentially frees the Board of Directors of a corporation from possible liability for decisions that result in harm to the corporation. The harm here is monetary losses due to a business decision. Cyber Security

Reliability Standards, however, are unrelated to business decisions. Cyber Security standards are intended to protect the entire national electric grid from cyber threats. A breach in cyber security of one utility could potentially disable the entire national electric grid, not just the geographical region served by that utility. Thus, it is an issue of National Security, rather than business judgment. The Business Judgment Rule should accordingly be removed from the CIP standards.

The standard guideline for satisfaction of the business judgment rule can be summarized as follows. Directors in a business should:

- not involve self-interest;
- act on an informed basis;
- act in good faith ; and
- act in the best interests of the corporation

All four of these points are matters that are ultimately open to interpretation. They all deal with business, not security, decisions. Implementing a Cyber Security program prescribed by a CIP standard will cost every entity an amount of money. However, in reliance on the fourth of the above criteria, directors acting in the best interest of their corporations could argue that spending the extra money needed to comply with a CIP standard is not "in the best interests of the corporation."

As mentioned above, each of the proposed CIP standards contains the Business Judgment Rule. An example of the problem that this creates can be seen in one of the requirements of CIP-007-1, which states that anti-virus software must be implemented. However, requirement 4 (R4) in this standard also states that anti-virus software must be implemented where "technically feasible." Using the Business Judgment Rule, an entity

can ignore installing any anti-virus software if the cost of modifying its system to accept an anti-virus program is high. However, a failure to install such software by one company could have a serious adverse impact on the entire Bulk Power System, as well as on all other entities that are fully compliant with the CIP Reliability Standards.

If an entity is allowed to rely on the Business Judgment Rule to ignore a strong verification system at access points when contacted from outside the ESP, it places the entire Bulk Power System at risk in case of an attack. Thus, that entity does not only place itself at risk in relying on the business judgment rule. The Business Judgment Rule should be accordingly removed from all CIP standards.

B. Applicability of the Proposed Standards

The CIP Reliability Standards list the following 11 categories of Responsible Entities in their applicability sections: Reliability Coordinators, Balancing Authorities, Interchange Authorities, Transmission Service Providers, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, Load Serving Entities, NERC, and Regional Reliability Organizations.

In its comments in Docket No. RM06-16-000, the CPUC argued that the Electric Reliability Organization ("ERO") and the Regional Reliability Organizations ("RRO") should not be subject to those reliability standards. However, the CPUC believes that the ERO and the RROs should be subject to the CIP standards.

It is important that if an RRO and the ERO have a cyber connection with an applicable entity, and entity is connected to the Bulk Power System, then the RRO and ERO need to adhere to the CIP Reliability Standards. The CPUC agrees with the "weak link" scenario that FERC Staff has suggested. RROs are connected to the users, owners

and operators of the Bulk Power System. If RROs do not adhere to the CIP standards, they can become a weak link whose failure could cause serious harm to the Bulk Power System. Accordingly, the CIP standards need to apply to all entities directly or indirectly connected to the Bulk Power System.

Finally, there is an issue with the applicability of the CIP standards to small entities. In the proposed standards that were the subject of FERC's NOPR in RM06-16-000, certain exceptions existed for the owners of small generating and transmission facilities on the grounds that such entities would have no impact on the Bulk Power System, even though they were connected to that system.

This connectivity is the crux of the problem in the case of the proposed CIP standards. Even though an entity is deemed to have no impact on the Bulk Power System, it is still connected to the system, and thus the CIP standards must apply to it. Regardless of the size of the entity or its impact on the system, the CIP standards need to apply to all entities directly or indirectly connected to the Bulk Power System.

The "weak link" concept discussed just above in connection with the RROs and ERO also applies to these small entities. Any entity, regardless of size, that is connected to the Bulk Power System and not subject to cyber security standards is a weak link. Such an entity possesses an unprotected gateway to the Bulk Power System, and such a gateway could lead to a catastrophic event. A cyber attacker could pick the weakest link, rather than the entity with the most connections to the system. The size of an entity is therefore irrelevant to the potential damage to the grid caused by a cyber attack. Consequently, every entity that is directly or indirectly connected to the Bulk Power System, regardless of size, needs to adhere to the CIP Reliability Standards.

IV. COMMENTS ON SPECIFIC PROPOSED STANDARDS

A. CIP-002-1 Critical Cyber Assets

This standard deals with identifying all Critical Assets. It requires entities to maintain an accurate inventory of Critical Assets, including Critical Cyber Assets that are accessible through routable protocols or by dial-up. The standard states that the list of assets should be reviewed when any Critical Asset has been added, removed, or modified. The list of assets must be approved by senior management and reviewed every year. The successful implementation of the CIP Reliability Standards relies on this proposed standard. All Critical Assets must be identified; misidentifying one asset would render the CIP standards useless.

The CPUC believes that calling for a risk-based assessment methodology to identify Critical Assets is a good start. However, more direction on what constitutes a risk-based methodology is needed. Guidelines are needed to spell out what a proper risk-based methodology would consist of. This is especially critical for small entities that have no impact on the Bulk Power System.

Finally, in updating the list of Critical Assets after an asset has been added, removed, or modified, there is no time window restriction for the completion of this update. UA 1200 has a 90 day limit for an update, and CIP-002 needs something similar. Since most of the Entities in the industry are familiar with UA1200, the CPUC suggests that a similar 90 day limit for an update be incorporated into CIP-002.

B. CIP-003-1 Security Management Controls

This standard calls on entities to document and implement a cyber security policy that defines a structure of relationships and decision-making processes. A key requirement

of this standard is the implementation of an Access Control program. The program calls for maintaining a list of personnel authorized to grant access to Critical Cyber Assets. For each authorized user, the list shall include a name, title, phone number, and list of assets to which access is being granted. The program that accesses Critical Cyber Assets is limited to authorized personnel.

The CPUC is pleased to see that this standard calls for the appointment of a senior manager to manage the implementation of the CIP standards and the implementation of an Access Control program. However, the provision in this standard that the senior manager appointed to manage and implement the CIP standards can authorize any exception to the cyber security policy causes concern. The manager can either explain and document why the exception is necessary, or issue a statement accepting risk. All exceptions must be documented within 30 days of approval and all exceptions must be reviewed on an annual basis to see if the exceptions are still valid.

The CPUC agrees with FERC Staff's assertion that "this requirement may act as a disincentive for upgrading to a control system that can meet all of the features of the security policy without exceptions" and that "for interconnected control systems of various entities, an acceptance of a cyber risk by one entity is actually an acceptance of risk for all of those connected entities because the entity that initially accepted the risk is now the weak link in the chain."

Such exceptions should not be allowed. These standards are intended to be mandatory, not optional. Allowing for exceptions may endanger the entire Bulk Power System, not just a given entity's customer base.

Another CPUC concern with CIP-003-1 deals with the access granted to Critical

Assets to authorized personnel who have been dismissed or have left the employ of a company. The standard does not state how soon after such an event the access granted to this person should be revoked. The list of personnel having access to Critical Assets needs to be revised once a year, but this may imply that a person that was terminated 10 days after such a review will still have access to Critical Assets for another year. After a person with access has left, his/her access privileges should be terminated immediately.

C. CIP-004-1 Personnel and Training

The CPUC agrees with the requirements of CIP-004-1. This standard states that entities should establish security awareness programs for their employees and conduct annual security training. All personnel, internal or external, who have access to Critical Cyber Assets, should undergo a personnel risk assessment. The entities will continuously track the Critical Cyber Assets to the users that have access. Access controls should be updated upon the termination or transfer of personnel.

However, as mentioned above in connection with CIP-003-1, there is no limitation as to how quickly this update should take place. The standard should be amended to require immediate updates when an employee is transferred, retires or is terminated.

D. CIP-005-1 Electronic Security Perimeters

This standard requires that an entity identify the Electronic Security Perimeter surrounding its Critical Cyber Assets. Entities should recognize and securely control all access points to this perimeter. Non-critical assets in the perimeter, as well as assets used for monitoring and access control, should be given the same protection as Critical Cyber Assets, to make certain that they do not become the gateway to a cyber attack.

The CPUC believes that this is a sound standard. Access controls should be

implemented at all access points to the network. Further, the caveat of "technical feasibility" in the NERC-proposed standard is inappropriate. The CPUC agrees with FERC Staff's assertion that "such technology currently exists" and implementation by every entity should be feasible.

The standard prescribes that only those ports and services required for normal or emergency operations should be enabled, while all others should be disabled. The access control, including the authorization process and authentication method for each access point, should be documented. Access should be monitored twenty-four hours a day, seven days a week, and disturbances and attempts at unauthorized access should be identified. All entities should conduct vulnerability assessments of their access points, scanning to verify that only the proper ports and services are enabled. Moreover, access from outside the Electronic Security Perimeter should require strong verification, such as digital certificates or two-factor authentication. Such two-factor authentication is not uncommon in the business world. Such a system is virtually impenetrable and something similar should be required in connection with the implementation of the CIP Reliability Standards.

E. CIP-006-1 Physical Security of Critical Cyber Assets

This standard deals with physical security of the Critical Cyber Assets identified in CIP-002-1. Entities should establish and document all physical access controls, such as card keys, special locks and on-site security personnel. A physical security plan must be created and maintained. The plan must be approved by senior management.

The CPUC finds this standard sound except for one issue. The standard does not require a plan in the contingency of a physical security breach. A succinct guideline for such a contingency plan needs to be incorporated into this standard.

F. CIP-007-1 System Security Management

This standard calls on the entities to implement system security controls to detect, deter and avert the failure or compromise of Critical Cyber Assets by mistake, misuse or malevolent activity. This standard has many positive aspects, including a call for testing the Critical Cyber Assets to ensure that the appropriate patches, service packs and vendor releases have been installed.

However, the mandated use of an anti-virus software and file integrity monitoring tools is essential in connection with the implementation of this standard. Requirement 6.1 states that entities should implement account management methods to enforce access authentication and to keep users accountable for their activity. Another requirement calls for network activity monitoring and alerts to be issued when Cyber Security Events are detected. Also, the standard requires that account passwords should include at least six characters, including alpha-numeric and special characters. A frequent change in passwords is stressed. As with CIP-005-1 above, a two-factor authentication program/system would be ideal in such instances.

The basic approach set forth in this proposed standard is reasonable. However, two problematic phrases are prevalent throughout the standard: “acceptance of risk” and “technically feasible.” The CPUC agrees with FERC Staff that the option of acceptance of risk should be eliminated from all the CIP standards. Moreover, common logic would dictate that in the instances where the phrase “technically feasible” appears, feasibility is actually possible. In this standard, this phrase appears, for example, in connection with the use of anti-virus software and malicious software prevention tools. However, anti-virus software should be technically feasible on any system; there are many different types of

anti-virus programs in the market that are compatible with virtually every available system. Accordingly, the phrase, "technically feasible," should be deleted from this standard except in those cases where the technology being discussed is experimental, still in development or not actually available on the market.

G. CIP-008-1 Incident Reporting and Response Planning

This standard states that entities should develop and maintain Cyber Security Incident response plans. The CPUC believes that this is a clear, concise and complete standard.

H. CIP-009-1 Recovery Plans for Critical Cyber Assets

The goal of this standard is to develop and document recovery plans that define the roles and responsibilities of responders. Plans should be tested through recovery exercises once a year and plans should include methods and procedures for backup and restoring Critical Cyber Assets.

The language of this proposed standard prescribes all the needed steps. However, the CPUC believes that in order to fully identify potential problems, an entity needs to conduct a full operational exercise. Only a full operational exercise can assure that all potential problems have been identified. The standard does not require entities to perform a full operational exercise, but it should.

V. CONCLUSION

For all the foregoing reasons, FERC should carefully review the language of the CIP Reliability Standards that NERC filed. FERC should be skeptical of the supposed usefulness and importance of allowing an entity to use the Business Judgment Rule to accept the risk of non-compliance. FERC should also apply the proposed rules to all

entities, regardless of size. Making sure that every entity connected to the Bulk Power System conforms to the CIP Reliability Standards will strengthen cyber security. Finally, the words "technically feasible" should be removed from each of the proposed CIP Standards unless there is a serious question about the actual feasibility of a requirement being imposed.

Dated: February 12, 2007

Respectfully submitted,

RANDOLPH L. WU
MARY F. McKENZIE
HARVEY Y. MORRIS
LAURENCE G. CHASET

By: *Laurence G. Chaset*
_____

Laurence G. Chaset
505 Van Ness Avenue
San Francisco, CA 94102
Phone: (415) 355-5595
Attorneys for the Public Utilities
Commission of the State of California

CERTIFICATE OF SERVICE

I hereby certify that I have this day caused the foregoing document to be served upon all known parties in this proceeding by e-mail upon each party identified in the official service list compiled by the Secretary in this proceeding.

Dated at San Francisco, California, this 12th day of February, 2007.

/s/ Laurence G. Chaset

Laurence G. Chaset

Submission Contents

coverltrSalasRM0622CIP.doc..... 1-1

RM0622CIPcomms.doc..... 2-15