UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

STAFF PRELIMINARYASSESSMENT FOR	**)**	
	)	**Docket No. RM06-22-000**
EIGHT CYBER SECURITY STANDARDS	**)**	
FOR THE BULK-POWER SYSTEM	**)**	

COMMENTS OF
THE ISO/RTO COUNCIL

In accordance with the Commission's Notice of Comment Period issued on December 11, 2006 (the "Notice") the ISO/RTO Council ("IRC")[1] submits comments on the "Staff Preliminary Assessment" ("Staff Assessment") issued concurrently with the Notice.[2] The Commission requests industry comments on the eight proposed Critical

---

[1] The IRC is comprised of the Independent System Operator operating as the Alberta Electric System Operator ("AESO"), the California Independent System Operator Corporation ("CAISO"), Electric Reliability Council of Texas ("ERCOT"), the Independent Electricity System Operator of Ontario ("IESO"), ISO New England Inc. ("ISO-NE"), Midwest Independent Transmission System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM") Southwest Power Pool, Inc. ("SPP") and New Brunswick System Operator ("NBSO"). The IESO, AESO and NBSO are not subject to the Commission's jurisdiction and their endorsement of these reply comments does not constitute agreement or acknowledgement that either can be subject to the Commission's jurisdiction. The IRC's mission is to work collaboratively to develop effective processes, tools and standard methods for improving competitive electricity markets across North America. In fulfilling this mission, it is the IRC's goal to provide a perspective that balances reliability standards with market practices so that each complements the other, thereby resulting in efficient, robust markets that provide competitive and reliable service to customers.

[2] *Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, December 11, 2006. Docket RM06-22-000.

Infrastructure Protection (CIP) Reliability Standards (CIP-002-1 through CIP-009-1) ("CIP standards") that the North American Electric Reliability Corporation filed with the Commission on August 28, 2006[3] for approval under section 215 of the Federal Power Act ("FPA"). As this is the first step in a larger rulemaking, the IRC will limit its comments specifically to the inquiries raised by the Commission Staff in its Staff Assessment. As noted below, Staff has raised important issues concerning the appropriate scope of the CIP standards and the applicability of the standards. For purposes of these specific comments, the IRC, as a group, will be commenting only from the perspective of a control center environment that is typical to an ISO or RTO organization. [4]

The IRC recognizes and appreciates the comprehensive review of the standards by the Commission Staff and finds its assessment constructive and helpful. The IRC offers the following comments to provide additional information to assist the Commission Staff in its assessment.

I. COMMENTS

1. Business Judgment

FERC Staff raised a concern regarding a "one size fits all" approach NERC has applied to its proposed Standards. Staff also raised concerns with that aspect of the

---

[3] The August 28, 2006 filing ("August 2006 Filing") was submitted by the North American Electric Reliability Council and its affiliate, the North American Electric Reliability Corporation, which is the Electric Reliability Organization ("ERO") (collectively, "NERC").

[4] Individual IRC members may file separate comments of their own addressing the scope of the proposed Standards.

proposed NERC Standards that would allow Responsible Entities to use "reasonable business judgment" when interpreting and applying the CIP Reliability Standards in recognition of "the differing role of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of assets needed to manage reliability and the risks to which they are exposed." [5] Staff raised similar concerns with language in the standards which limit their application "when technically feasible".[6]

The IRC shares Staff's concern with trying to arrive at a one size fits all standard. However, the IRC believes that this is precisely the reason to ***retain*** rather than eliminate the "business judgment" and "technically feasible" language in the proposed standards. The fact that there are many different cyber environments and technologies argues for retention of these important caveats (with one possible clarification noted below). For example, dissimilar technologies are deployed across ISO/RTO entities such that what may be technically feasible for one may not be practically feasible for another. In addition, there are often multiple mitigation strategies available and the application of reasonable business judgment is required to select the most appropriate strategy for implementation. The dissimilarity of deployed technology becomes even more significant when one moves out of the control center environment and into the generation and substation facilities. It is simply not possible to write a "one size fits all" rule because such a rule would ignore the multitude of systems as well as the different threat levels that they impose to the grid.

---

[5] Staff Assessment, p. 10

[6] Staff Assessment, p. 27

Contrary to the implication of the Staff Assessment on this point, the IRC believes that incorporation of the terms "reasonable business judgment" and "technically feasible" into a CIP standard will still ensure that the standard is enforceable. For one, as NERC indicates[7], NERC-certified auditors, schooled in different applications, will be providing key information to the audited party as well as to the ERO and the Commission regarding what practices are within the zone of reasonableness and constitute acceptable business practices in this area. A growing record of industry practices will be available for the Commission to call upon in order to judge, in a particular case, whether an action is within or outside that zone. The term "reasonable" is an important and widely used modifier to "business judgment", and the availability of independent NERC-certified auditing can ensure that the term "reasonable" is appropriately applied in a given context. By contrast, should the Commission attempt to prescribe specific practices in lieu of adopting the "reasonable business judgment" and "technically feasible" language, it runs the risk of establishing standards which are inappropriately inflexible and unable to cover all situations. Such prescriptive standards may ultimately fall of their own weight as a result of the regulatory process being unable to keep up with rapidly changing technological developments as well as the multitude of different environments to be assessed and addressed within the standard. For these reasons, the IRC urges the Staff to support inclusion of the "reasonable business judgment" and "technically feasible" language in the proposed rule.

---

[7] See *NERC Compliance Monitoring and Enforcement Program*, draft dated November 3, 2006, www.nerc.com

That being said, the IRC is sensitive that one could read the "reasonable business judgment" language, which admittedly arises out of a corporate law context, to imply that profit and loss implications should be the deciding factor in determining an appropriate level of compliance. Clearly, there is a greater public interest in ensuring a reliable grid. As a result, it may be appropriate to link the exercise of "reasonable business judgment" to achievement of the overall goal, i.e., ensuring protection of critical infrastructure to ensure a reliable bulk power grid. Requiring the overall objective to be met when applying the "reasonable business judgment" standard would alleviate any concern that the standard would allow profit and loss factors to trump the need for adequate protection of critical infrastructure.

2. Security Management Controls

The Commission Staff notes that Requirement R1 of CIP-003-1 requires a Responsible Entity to "document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets."[8] Staff further notes that Requirement R3 requires a Responsible Entity to document every instance in which the Responsible Entity cannot conform to the security policy and that this requirement allows for broad discretion.[9]

The IRC believes that providing latitude for management to document exceptions to the Responsible Entity's established policies and procedures, select alternative and mitigating solutions, and ultimately accept residual risk is wholly appropriate.

[8] Staff Assessment, p. 19

[9] Staff Assessment, p. 20

Exceptions are permitted where the Responsible Entity cannot meet the requirements of the cyber security policy that implements the CIP Standards. However, consideration of mitigation and/or acceptance of risk should occur and be appropriately documented as a part of the approval by the Senior Security Manager. Such documentation should also be subject to annual review by the Responsible Entity.

3. Incident Reporting and Response Planning

The Commission notes that Requirement R1.6 of CIP-008-1 requires annual testing of the Cyber Security Incident Response Plan, which could range from a "paper drill" to a full operational exercise. The Commission Staff requested comment as to whether full operation exercises should be required by the Standard.[10]

The IRC does not believe that full operational exercises should be required within any prescribed timeframe. Table-top exercises can be constructed in such a manner that the response team can demonstrate knowledge of assigned responsibilities and response methodologies such that a full operational exercise is not necessary. The IRC believes that table-top exercises are sufficient and can be conducted at least annually.

4. Documentation

The Commission Staff expresses concern relating to requirements within several standards that a ninety day timeframe for updating documents is excessive.[11]

The IRC agrees that updates to documents required by the CIP standards generally can be performed sooner than the currently required 90 days. The timely

[10] Staff Assessment, p. 37

[11] Staff Assessment, pp. 27, 38

updating of required documents should be a formal component of any assessment or review process. This is particularly applicable to post-mortem assessments of exercises, or actual events, and the documentation of, and timely application of, lessons learned.

5. Physical Security of Critical Cyber Assets

The Commission notes that CIP-006-1 requires access logs to be maintained for 90 days, while outage records regarding access controls, logging and monitoring must be kept for at least one year.[12] Requirement R5 of CIP-006-1 requires that logs related to reportable incidents be retained longer than the minimum of 90 days. The Commission Staff believes that document retention should not be limited to reportable incidents and that all physical access logs should be retained for at least one year.[13] The Staff questions whether consideration should be given to testing the higher level of critical physical security mechanisms and systems more frequently, with testing and maintenance records maintained for the full 3 year testing cycle. [14]

The IRC believes that the required retention of logs for 90 days is sufficient. After 90 days, the value of log data is generally diminished and there is no reasonable security benefit to retaining the data longer than the 90 day period. However, the IRC acknowledges that the requirement to retain both physical and electronic log data specific to a cyber security incident for three years is appropriate.

---

12 Staff Assessment, p. 28

13 Staff Assessment, p. 30

14 Staff Assessment, p. 42

6. Monitoring of Logs

The IRC believes that automated log monitoring, analysis, and alerting, satisfies the requirement for review of logs within 90 days. In this regard, logs can be reviewed more frequently than 90 days. Requiring additional manual reviews on top of automated reviews would add little value and would be unnecessarily burdensome given the significant volume of log data in control centers such as those operated by ISOs and RTOs.

7. Personnel and Training

The Commission notes that Requirement R4 of CIP-004-1 directs a Responsible Entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets." However, the lists do not serve to keep un-cleared personnel from Critical Cyber Assets prior to completion of a personnel risk assessment. The Commission Staff also notes that it may be appropriate for the Standard to include a provision that would direct a Responsible Entity to establish a categorization of access according to the exposure level or frequency of exposure to Critical Cyber Assets.[15]

The IRC agrees that a personnel risk assessment and appropriate security training should be completed prior to granting access to critical cyber assets.[16] The IRC does not agree that establishing category levels of access is necessary. There are no significant

---

[15] Staff Assessment, p. 24

[16] The specific applicability of this in Alberta is being reviewed to ensure consistency with provincial and federal laws.

levels of risk differences between critical cyber assets. They are all relatively equal in their criticality to the Bulk Electric System.

8. Reporting of Critical Cyber Asset Security Incidents

The Commission notes that CIP-008-1 requires that the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) be notified of any reportable cyber security incident, and that there is no defined time frame for sending the report.[17] It also notes that the Requirement does not provide definition on the characteristics of a "reportable incident".[18]

The IRC generally does not agree that the Standards' requirements should identify any criteria, thresholds, or time requirements for reporting of critical cyber asset security incidents. The IRC believes that any requirements should be determined by ES-ISAC, and the requirement to report such incidents to the ES-ISAC is sufficient. We would therefore look to the ES-ISAC to define appropriate reporting requirements, and be able to make time-sensitive adjustments to such criteria as particular events may dictate.

9. Implementation Plan Compliance

The Commission notes that Responsible Entities will not be required to be "Auditably Compliant", as defined by the Implementation Plan until the second quarter 2009 or second quarter 2010. It also notes the possibility of assessing a Responsible Entity's level of compliance prior to achieving its full "Auditably Compliant" status. The

---

[17] Notification by Alberta would be subject to alignment with provincial and federal security laws and interests.

[18] Staff Assessment, pp. 36-37

Commission Staff seeks comment whether it would be beneficial to audit a Responsible Entity at the "Begin Work" and "Compliant" stages even though it may not have the full accumulation of twelve months of records available.[19]

The IRC agrees with the Commission's assessment that a process for performing an advisory assessment may actually be of benefit to organizations. Such advisory reviews could be offered by the Regional Entities with the clear understanding that the reviews will not result in penalties, or be used to determine areas of investigation for the "compliance audit". Because such reviews would only occur between now and the deadlines for compliance audits, the IRC recommends that the team that performs the advisory review be different from the team that performs the audit and that the result of the review remain confidential between the review team and the entity.

10. Applicability

The Commission notes that only a few proposed Reliability Standards are explicitly applicable to NERC. The Commission Staff seeks comment on whether CIP Reliability Standards should apply to NERC and, if so, the appropriate mechanism by which to direct such compliance.[20]

The IRC recognizes that NERC plays an important role supporting the Reliability Coordinators (RC) in that it provides key decision systems used by the RC. As such, it is vital that NERC be subject to the CIP standards. Further, the fact that NERC out-sources such systems to a third-party service provider, such as the Interchange Distribution

---

[19] Staff Assessment, p. 11

[20] Staff Assessment, p. 13

Calculator, is immaterial. The out-source provider should be contractually compelled to comply with the CIP Standards with NERC ultimately responsible for non-compliance. Any compliance audits of NERC should be conducted by parties independent of NERC itself.

III. CONCLUSION

For the reasons set forth above, the IRC requests that the Commission consider the foregoing comments in the development of the Notice of Proposed Rulemaking which the Commission will issue with its proposal on each CIP standard.

Respectfully submitted,

/s/Craig Glazer
/s/Jennifer Bellwoar
Craig Glazer
Vice President–Federal Government Policy
Jennifer A. Bellwoar
Senior Counsel
PJM Interconnection, L.L.C.
1200 G Street, N.W., Suite 600
Washington, D.C. 20005

/s/Stephen Kozey
Stephen G. Kozey
Vice President and General Counsel
Midwest Independent Transmission
System Operator, Inc.
701 City Center Drive
Carmel, Indiana 46032

/s/Raymond Hepper
Raymond W. Hepper
Vice President and Assistant General
Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040

/s/Anthony Ivancovich
Anthony Ivancovich
Acting Vice President of Legal Affairs
California Independent System
Operator Corporation
151 Blue Ravine Road
Folsom, California 95630

/s/Kim Warren
Kim Warren
Manager, Regulatory Affairs
Independent Electricity System
Operator of Ontario
655 Bay Street, Suite 410
Toronto, Ontario, MSG-2K4 Canada

/s/Robert Fernandez
Robert E. Fernandez
Vice President and General Counsel
Elaine Robinson
Director of Regulatory Affairs
New York Independent System
Operator, Inc.
290 Washington Avenue Extension
Albany, N.Y. 12203

/s/Diana Pommen
Diana D. Pommen
Director Business Operations
Alberta Electric System Operator
Calgary Place
2500 330 – 5th Avenue SW
Calgary, AB T2P 0L4

/s/ Michael Grable
Michael Grable
Assistant General Counsel
Electric Reliability Council of Texas
7620 Metro Center Drive
Austin TX 78744

/s/Stacy Duckett
Stacy Duckett
General Counsel & Corporate Secretary
Southwest Power Pool, Inc.
415 North McKinley
#140, Plaza West
Little Rock, Arkansas 72205-3020

/s/ Kevin C. Roherty
Kevin C. Roherty
Secretary and General Counsel
New Brunswick System Operator
77 Canada Street
Fredericton, NB E3B 5G4