

LAW OFFICES
BALLARD SPAHR ANDREWS & INGERSOLL, LLP
601 13TH STREET NW, SUITE 1000 SOUTH
WASHINGTON, DC 20005-3807
202-661-2200
FAX: 202-661-2299
WWW.BALLARDSPAHR.COM

PHILADELPHIA, PA
BALTIMORE, MD
BETHESDA, MD
DENVER, CO
LAS VEGAS, NV
LOS ANGELES, CA
PHOENIX, AZ
SALT LAKE CITY, UT
VOORHEES, NJ
WILMINGTON, DE

October 5, 2007

VIA ELECTRONIC FILING

Honorable Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

**Re: Mandatory Reliability Standards for Critical Infrastructure
Protection, Docket No. RM06-22-000;
Comments of ISO New England Inc.**

Dear Ms. Salas:

Transmitted electronically for filing in the above-referenced dockets are the
Comments of ISO New England Inc.

If there are any questions concerning this filing, please call me at (202) 661-2212.

Very truly yours,

/s/ Daniel R. Simon

Daniel R. Simon
Counsel for
ISO New England Inc.

Enclosure

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Mandatory Reliability Standards for)
Critical Infrastructure Protection)

Docket Nos. RM06-22-000

COMMENTS OF ISO NEW ENGLAND INC.

Pursuant to the Notice of Proposed Rulemaking (“NOPR”) issued by the Federal Energy Regulatory Commission (the “Commission”) in the above-captioned proceedings,¹ ISO New England Inc. (“ISO-NE”) respectfully submits these comments.

I. BACKGROUND

ISO-NE is the private, non-profit entity that serves as the Regional Transmission Organization (“RTO”) for New England. ISO-NE administers the New England energy markets and operates the regional bulk power system (*i.e.*, those facilities located in the New England region) pursuant to the ISO New England Inc. Transmission, Markets and Services Tariff, FERC Electric Tariff No. 3 (the “ISO-NE Tariff”) and Operating Agreements with the New England transmission owners. In its capacity as the RTO for New England, ISO-NE has the responsibility to protect the short-term reliability and plan for the long-term reliability of the control area, a six-state region that includes approximately 6.5 million businesses and households.

II. COMMENTS

The eight Critical Infrastructure Protection (“CIP”) Reliability Standards at issue here are intended to help maintain Bulk-Power System reliability. It is appropriate to identify those

¹ Mandatory Reliability Standards for Critical Infrastructure Protection, Notice of Proposed Rulemaking, 72 Fed. Reg. 43,970 (Aug. 6, 2007) (the “NOPR”).

functions and physical assets (Assets) that play a vital role (Critical Assets) in sustaining a reliable Bulk-Power System and interconnections between systems. It is therefore prudent to protect those cyber assets identified as critical to the reliable performance of said Critical Assets (critical functions and critical physical assets).

A. Mutual Distrust

The NOPR introduces the principle of “Mutual Distrust” when it states:

Regarding our concern about small entities becoming a gateway for cyber attacks, some commenters argue that the Commission should not focus on cyber connections to determine applicability of the CIP Reliability Standards. Others state that it would be uncommon for a small entity to cause an adverse impact upon the grid. The Commission’s reliance upon the NERC registration process to determine the applicability of the CIP Reliability Standards is in part based upon our expectation that industry will use the “mutual distrust” posture discussed below regarding CIP-003-1. The term “mutual distrust” is used to denote how these “outside world” systems are treated by those inside the control system. A mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates.²

The NOPR goes on to propose “to direct the ERO to modify Reliability Standard CIP-003-1 to provide direction regarding the issues and concerns that a ‘mutual distrust’ posture must address to protect the control system from the ‘outside world.’”³ The NOPR explains that “[a]n architecture with a mutual distrust posture could involve various hardware or software mechanisms or manual procedures to restrict and verify access to the control system from these

² NOPR at P 28.

³ *Id.* at P 147.

outside sources. Examples include: firewalls; data checking software(s); or procedures for manually implementing a connection to allow a vendor to perform maintenance work.”⁴

Applying a principle of mutual distrust as a rationale for determining when to protect cyber assets is a strategic decision which, as pointed out by the Commission, is an appropriate consideration in designing a secure system architecture. But, it does not work well as a measurable requirement. As criteria for identifying critical cyber assets, mutual distrust itself is not a factor in making a cyber asset critical. Further, in creating the Cyber Security Standards, the ERO already has established that critical cyber assets will be protected. Either Responsible Entities are compliant or they are not, mutual distrust notwithstanding.

Therefore, ISO-NE asks that the Commission omit any direction to the ERO to address the concept of Mutual Distrust.

B. Implementation

The NOPR proposes “to direct that the ERO develop a self-certification process with more frequent certifications, either tied to target dates in the schedule or perhaps quarterly or semi-annual certifications”⁵ and “to direct the ERO to add a cyber security assessment to NERC’s existing readiness reviews.”⁶ ISO-NE believes these directives are unnecessary. NERC already has implemented a formal, detailed, and annual self-certification process through the Regional Entities. NERC also has already begun addressing the Cyber Security Standards in its Readiness Reviews.

⁴ *Id.* at P 147 n.81.

⁵ NOPR at P 48.

⁶ *Id.* at P 49.

ISO-NE asks the Commission to omit any direction to the ERO for more frequent self-certifications and reviews. These requirements would merely divert the ISO's limited resources from actual implementation activities.

C. Issues Presented by Terminology

ISO-NE supports the Commission's proposals to eliminate all references to the terms "Reasonable Business Judgment"⁷ and "Acceptance of Risk."⁸ These terms provide no measurable value to any of the requirements in the standards, and they appear to be open-ended caveats that are susceptible to abuse. ISO-NE supports codifying the practice of exceptions to be limited to those requirements that explicitly invoke "technical feasibility," independent of business judgment, as a compliance factor. Reporting such exceptions to Regional Entities can play a useful role in identifying standards and requirements with frequent implementation issues that may necessitate modification to a standard or some of its requirements.

ISO-NE, however, has two concerns regarding such reporting of exceptions. First, detailed technical descriptions of the exceptions should not be passed to either the Regional Entities or to the ERO. Such information would be considered potential vulnerability information about critical cyber assets, or their environments, and should be protected by the Responsible Entity as critical cyber asset information under CIP-003-1, Requirement 4. Second, neither the Regional Entity nor the ERO should have oversight approval of exceptions. It is highly unlikely that either the Regional Entity or the ERO will have the resources with the breadth of necessary skills to evaluate the broad spectrum of technical cyber configurations that are implemented throughout the industry. Even if the appropriate skilled resources were

⁷ *Id.* at P 58.

⁸ *Id.* at PP 77 & 86.

available, providing sufficient data for such evaluations would require the submission of critical cyber asset information, which raises again our concern regarding protection of such information under CIP-003-1, R4.

D. Data

The NOPR raises the issue of data as a critical asset:

Moreover, we note that the definition of “critical cyber assets” encompasses data. Thus, marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process that data, would be considered critical cyber assets subject to the CIP Reliability Standards. Therefore, the Commission proposes to direct the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to include computer systems that produce the data.⁹

By definition, a critical cyber asset is comprised of 3 components: hardware, software, and data.¹⁰ ISO-NE agrees with the ISO/RTO Council comments that data by itself does not meet the definition of a critical cyber asset. However, the Commission is further viewing data as a potential critical asset. ISO-NE agrees with this view in concept, but believes that consideration of reliability data is already intrinsic to the process of evaluating assets (operational functions performed as well as physical assets) to determine their criticality. Such reliability data is “real-time data” and is highly transient as it passes through, and is presented by, such supporting critical cyber assets. Given that protection of critical cyber assets is already

⁹ *Id.* at P 114.

¹⁰ *Id.* at P 114 n. 69 (“The NERC Glossary defines ‘Critical Cyber Asset’ as ‘Cyber Assets essential to the reliable operation of critical assets.’ It defines ‘Cyber Assets’ as ‘programmable electronic devices and communication networks including hardware, software, and data.’ Therefore, marketing data or other system data that are essential to the proper operation of the critical asset may confer critical cyber asset status to those data and the computer systems that process them.”).

being addressed, the protection of the data component of a cyber asset during its instance of viability as useful reliability data is satisfied. To address a broader focus of data protection would expand the scope of the current CIP Standards. Such a focus deserves considerable review and discussion, which has not yet been addressed. It could also impact the ability of the current set of standards to maintain a one-size-fits-all approach. If the Commission continues to have concern regarding data protection from a broader view, ISO-NE recommends this be considered in a future proceeding that openly discusses whether it would be appropriate to direct the development of one or more NERC standards to address data protection with consideration to Control Centers and/or Remote Reliability Facilities respectively.

ISO-NE is also concerned about the reference to “marketing data.” With respect to reliability, marketing data is not required by ISO-NE to maintain its Bulk-Power System. On occasion during emergencies, and while perhaps rare, ISO-NE has invoked its authority and capabilities to suspend market activity to maintain a reliable grid without regard to market conditions. To this extent, ISO-NE does not consider marketing data to be reliability data.

With respect to marketing data, such data and computer systems are already under heavy audit scrutiny with regard to SAS70 audits required on any business entity engaged in financial activities, such as the involvement of electric utilities engaged in the Bulk-Power System. ISO-NE believes it is not necessary and not reasonable to pursue separate standards that might cause compliance conflicts with existing audit requirement such as SAS70. ISO-NE therefore asks that references to Marketing and Other Data as a potential Critical Asset, and references to “the computer systems that process [it]” be omitted in the Final Rule.

E. Training

The NOPR proposes to “direct the ERO to modify the CIP-004-1 to clarify that the cyber security training programs required by Requirement R2 are intended to encompass training on

the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of the critical cyber assets.”¹¹ It appears that the Commission intends to address primary skilled-based training with this proposal. ISO-NE considers such training to be a business management decision to determine the level of skill training necessary for an individual, based on their functional task requirements and coordinated career goals. Such training is outside the scope of security training for access controls, monitoring, and incident response. ISO-NE requests that such training requirements be omitted from the Final Rule.

The NOPR also provides that “CIP-004-1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities.”¹² ISO-NE agrees with the ISO/RTO Council comments to the NOPR that training which addresses vulnerabilities is not appropriate for all individuals with access to critical cyber assets. Vulnerabilities associated with critical cyber assets and/or their security perimeters is highly sensitive and critical information. Such knowledge should only be in the hands of those with direct responsibility to administer the secure operation of the critical cyber assets and their security perimeters. ISO-NE therefore asks that the Final Rule direct the ERO to clarify that such information be protected under CIP-003-1 Requirement 4 and that such knowledge be shared on a need-to-know basis only.

F. Access Removal

The NOPR proposes to “direct that NERC develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor, or vendor no longer performs a function that requires authorized physical or electronic access to a critical cyber asset

¹¹ *Id.* at P 160.

¹² *Id.*

for any reason (including disciplinary action, transfer, retirement or termination).”¹³ ISO-NE has two concerns with regard to “disciplinary action” and “transfer.” First, the Commission should acknowledge that not all disciplinary action will arbitrarily warrant revocation of access privileges. Based on the severity of the disciplinary action, management should be allowed discretionary power in determining when revocation is warranted. Second, personnel transfers can at times require a protracted, transitional process, where there is good business reason to warrant the individual to retain access privileges after the formal transfer date. Most often this would be in cases where continued back-up support is appropriate while the individual’s replacement is being identified, or a personal risk assessment is conducted, and/or is trained and becomes familiar with new job responsibilities. Again, management should be allowed discretionary power in determining when revocation is warranted.

Therefore, ISO-NE requests that the Final Rule not impede management’s role and discretion in determining when access privileges are no longer necessary.

G. Logs

In CIP-005-1, Requirement 3.2 states:

Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

In CIP-007-1, Requirement 6 states:

The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible,

¹³ *Id.* at P 169.

implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

These Requirements expect that most Entities will be conducting automated log monitoring to detect and alert on any unauthorized or suspicious events. The requirement for manual review is intended only when automated monitoring tools are not technically feasible.

However, the NOPR (at paragraph 195) goes on to state:

The Commission is persuaded by the commenters that varied technologies and locations make setting a “one size fits all” frequency of access log review requirement difficult. However, the Commission believes that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Thus, regular manual review is beneficial.

It is ISO-NE’s view that automated log monitoring to detect and alert on any unauthorized or suspicious events is sufficient. ISO-NE has evaluated various tools to enhance its log monitoring practices. These evaluations were conducted against a subset of cyber assets similar to those that would be used to maintain an Electronic Security Perimeter (ESP) and those that would be found inside an ESP. The number of cyber assets involved was approximately one-third the number we expect to have involved in our production ESP environment. On a testing basis the evaluation was handling approximately eight thousand event records per minute, or 11.5 million records per day. On a fully implemented production basis, this would be in excess of 25 million event records a day. Any effort to routinely manually review logs of this

volume would be tantamount to looking for a needle in several hay stacks when you are not sure a needle even exists, and you might not even know what the needle looks like. Other than during a forensic investigation in response to an automated alert, any expectation of useful manual review on a routine basis is not reasonable.

ISO-NE therefore requests that the Commission limit the requirement for routine manual reviews to only those situations where automated monitoring and alerting tools are not technically feasible. However, ISO-NE does suggest that review of automated alerts should be frequent.

H. Defense in Depth

In discussing the “Defense in Depth” strategy, the NOPR appropriately points out that defense in depth “involves the layering of various defense mechanisms in a way that either discourages an adversary from continuing an attack or aids in early detection of cyber threats.”¹⁴ ISO-NE agrees with this strategy and believes that CIP-002-1 through CIP-009-1 together provide a defense in depth approach to protecting critical cyber assets. Collectively, the standards address requirements for personnel training and awareness, including exercises—the first and most effective line of defense. Additionally, the standards identify controls for both physical and electronic access through defensive perimeters; monitoring and alerting on those perimeters; access, monitoring, and alerting on critical cyber assets themselves; changes/updates to critical cyber assets; periodic assessment and appropriate remediation of these controls; response to security incidents; use of malicious software prevention tools; and protection of technical information about configuration and management of critical cyber assets.

¹⁴ *Id.* at P 14.

With respect to ESPs, however, the NOPR proposes “to direct the ERO to develop a requirement to implement a defensive security approach including two or more defensive measures in a defense in depth posture. This approach should not inhibit, but instead supplement the establishment of an electronic security perimeter.”¹⁵ ISO-NE believes such an additional requirement is unnecessary. Collectively, the standards already provide multiple defensive layers, such as measures for granting and revoking access privileges, as well as measures to authenticate access, monitor and alert on unauthorized or attempted unauthorized access, and procedures for response to alerts. With defensive measures and procedures already required at multiple layers, requiring an additional measure at a given layer is not necessary.

ISO-NE therefore requests that, in the Final Rule, the Commission not direct the ERO to develop an additional requirement addressing multiple measures within any given defense in depth layer.

I. Strong Authentication

Regarding CIP-005-1, the NOPR proposes to “add guidance to Requirement R2 by identifying examples of specific verification technologies that would satisfy compliance with the ‘strong controls’ in Requirement R2.4, such as digital certificates and two-factor authentication, while also allowing compliance by means of technically equivalent measures.” ISO-NE is slightly concerned regarding the phrasing of “‘strong controls’ ... such as digital certificates and two-factor authentication.” ISO-NE asks that the Final Rule ensure that “use of either digital certificates or two-factor authentication” constitute acceptable examples for strong authentication.

¹⁵ *Id.* at 181.

J. Change Management

Regarding CIP-007-1, the NOPR proposes “to direct the ERO to modify Requirement R1 and its subparts to require documentation of each significant difference between the testing and the production environments, and how each such difference is mitigated or otherwise addressed.”¹⁶ ISO-NE sees the term “significant difference” to be highly subjective and potentially burdensome without actually enhancing an Entity’s security posture. Therefore, ISO-NE requests that the Final Rule direct the ERO to provide greater clarity in this regard.

Regarding CIP-007-1, the NOPR proposes “to require that the ERO provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.”¹⁷ ISO-NE believes that, given the diversity of hardware and software implementation throughout the industry, providing more meaningful direction on “features, functionality, and vulnerabilities” is not feasible. No standard can evolve fast enough to keep-up with emerging and diverse technologies and newly discovered vulnerabilities. Therefore, ISO-NE requests that the Commission omit this proposal from the Final Rule.

K. Documentation Review/Update

Regarding CIP-007-1, the NOPR proposes “to direct the ERO to modify Requirement R9 to state that the changes resulting from modifications to the system or controls shall be

¹⁶ *Id.* at P 230.

¹⁷ *Id.* at P 260.

documented in a 30-day time period.”¹⁸ The NOPR makes a similar proposal for CIP-009-1 as well.¹⁹

ISO-NE is concerned that there is no clear indication of when the “30 day clock” would “start ticking.” Frequently the planning, engineering, and testing of such modifications could take longer than 30 days to implement, causing the documentation to still be out-of-date.

Therefore, ISO-NE requests that the Final Rule direct the ERO to clarify for both CIP-007-1 and CIP-009-1 that changes resulting from modifications to the systems, controls, and procedures shall be documented within 30 days of final implementation of said modifications.

L. Exercises

Regarding CIP-008-1:

[T]he Commission proposes to direct the ERO to revise the Reliability Standard to require responsible entities to perform a “full operational exercise” at least once every three years, or to fully document its reason for not conducting an exercise in full operational mode pursuant to the technical feasibility parameters discussed earlier in section II.A.5.b. Further, the Commission proposes to direct the ERO to provide guidance on the meaning of the term “full operational exercise.”²⁰

The NOPR makes a similar proposal for CIP-009-1.²¹

While ISO-NE has considerable concern regarding potential significant impact of conducting “full operational” exercises, this is in part due to a lack of clarity as to what constitutes such an exercise. ISO-NE thus supports the NOPR’s directive that the ERO provide

¹⁸ *Id.* at P 263.

¹⁹ *Id.* at P 308.

²⁰ *Id.* at P 286.

²¹ *Id.* at PP 303-304.

greater clarity as to the meaning of the term “full operational exercise.” As to whether to provide a definition of “full operational exercise” in the NERC Standard Glossary, it needs to be understood that what may qualify as such an exercise with regards to readiness of Bulk-Power System operations would be somewhat different from such an exercise with respect to a Cyber Security Incident Response Plan, or for IT back-up and recovery plans. Therefore, ISO-NE reserves further judgment of requirements for full operational exercises until additional clarity is provided.

M. Forensic Data Collection

The NOPR proposes to include reference and requirements regarding the collection of “forensic data.”²² ISO-NE agrees in part with the comments NERC submitted on this proposal. Further, “forensic analysis” is a skill used in the analysis of security incident data, the retention of which for three years is already addressed in CIP-008-1 for Security Incident Response. Also, CIP-005-1, CIP-006-1, and CIP-007-1 already require the retention of log data to support initial monitoring, analysis, and alerting of identified security incidents.

It is also our view that the broad-brush use of the term “forensic data” in the Blackout Report included all reliability incident data for post incident analysis. The scope is clear that these standards are limited to Cyber Security Incidents, and not all operational incidents impacting reliability. Therefore, ISO-NE believes the Reliability Standards already address this topic adequately, and it is therefore not appropriate to include in CIP-009-1. ISO-NE requests that any direction to the ERO regarding further collection of forensic data, or other operational reliability incident data, be omitted.

²² *Id.* at PP 297-298.

N. Backup and Restoration Processes and Procedures

The NOPR “proposes to instruct the ERO to modify this Reliability Standard [*i.e.*, CIP-009-1] to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes.”²³ The NOPR proposes similar requirements regarding backup procedure verification as well.²⁴

ISO-NE is concerned with these proposals. ISO-NE agrees that “regular procedures to ensure verification that backups are successful and backup failures are addressed” are acceptable if the intent is to review the back-up process. However, testing the actual back-up data is not realistic in most instances, insofar as the environment would literally have to be shut down and be restarted with the data in order to test it. In an emergency, the restored data is a good starting point for recovery, but for a test process, such activity would not be acceptable due to the impact on reliability and market systems. Therefore, ISO-NE requests that the Commission omit directing the ERO to make any changes to CIP-009-1 Requirements 4 and 5.

²³ *Id.* at P 312.

²⁴ *Id.* at P 319.

III. CONCLUSION

ISO-NE requests the Commission to consider the comments submitted herein.

Respectfully submitted,

/s/ Maria A. Gulluni

Maria A. Gulluni
Assistant General Counsel – Corporate
ISO New England Inc.
One Sullivan Road
Holyoke, MA 01040
(413) 540-4473
mgulluni@iso-ne.com

Dated: October 5, 2007