

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

**MANDATORY RELIABILITY STANDARDS)
FOR CRITICAL INFRASTRUCTURE) Docket No. RM06-22-000
PROTECTION)**

**COMMENTS OF THE ISO/RTO COUNCIL
ON THE NOTICE OF PROPOSED RULEMAKING**

The ISO/RTO Council (“IRC”)¹ respectfully submits these joint comments on the Commission’s Notice of Proposed Rulemaking on *Mandatory Reliability Standards for Critical Infrastructure Protection* (the “NOPR”).²

I. BACKGROUND

On July 20, 2007, the Commission issued the NOPR proposing approval of eight Critical Infrastructure Protection (“CIP”) Reliability Standards (“Reliability Standards”) developed by the North American Electric Reliability Corporation (“NERC”)³ and submitted to the Commission for approval. The eight new Reliability

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 comments does not constitute agreement or acknowledgement that either can be subject to the Commission’s jurisdiction. NERC-developed and FERC-approved reliability standards are not applicable in Alberta unless they have been subject to an internal Alberta process, including stakeholder consultation, AESO review and endorsement and approval of the Alberta regulator. This would apply to the CIP standards. 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 *Mandatory Reliability Standards for Critical Infrastructure Protection*, 120 FERC ¶ 61,077 (July 20, 2007) (the “NOPR”).

³ On February 3, 2007, the Commission issued Order No. 672 in which NERC was certified as the Electric

Standards were designated by NERC, and submitted to the Commission on August 28, 2006 as follows:

- CIP-002-1 – Cyber Security – Critical Cyber Asset Identification;
- CIP-003-1 – Cyber Security – Security Management Control;
- CIP-004-1 – Cyber Security – Personnel & Training;
- CIP-005-1 – Cyber Security – Electronic Security Perimeters;
- CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets;
- CIP-007-1 – Cyber Security – Systems Security Management
- CIP-008-1 – Cyber Security – Incident Reporting and Response Planning; and
- CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets.⁴

II. COMMENTS

The IRC commends the Commission and its staff for the thoughtfulness of the assessment of the Reliability Standards. We believe that the Commission’s proposals to approve all eight Reliability Standards and to approve NERC’s Implementation Plan and associated timelines for achieving compliance are necessary to ensure that Responsible Entities have taken adequate precautions against events that could jeopardize the reliability of the Bulk Electric System.

While we strongly support the Commission’s proposals overall, we are concerned about some details of the Commission’s comments and proposals. Accordingly, the IRC respectfully submits the following comments on the Commission’s proposed rulemaking.

Reliability Organization (“ERO”). *North American Electric Reliability Corp.*, 116 FERC ¶ 61,602 (ERO Certification Order), *order on reh’g & compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030 (January 2007).

⁴ NOPR at P 8.

These comments will address the following topical areas:⁵

- Critical Asset Determination---p. 4
- Role of Demand Side Aggregators---p. 6
- An Independent Determination of Critical Assets and Critical Cyber Assets—p. 7
- Scope of Application (Market Data)---p. 9
- Scope of Application (Compliance with Corporate Policies)---p. 11
- Proving Functionality of Changes and Back-ups---p. 13
- Training Program Requirements---p. 15
- Growth of Regional Entities---p. 16
- Approval of Exceptions by Third Parties---p. 18
- Specification of How Requirements are to be Met---p. 19
- Contractual Obligations for Outsourced Functions---p. 22

IRC SPECIFIC COMMENTS

A. Critical Asset Determination

In paragraph 115, the Commission proposes to modify NERC Requirement R1.2 to mandate that Responsible Entities explain their reasons for designating specific assets as Critical Assets or non-Critical Assets.⁶ In the IRC's opinion, depending on clarification of the Commission's intent and expectations, modification of this Requirement may not be necessary because Reliability Standard CIP-002, Requirement R1 already compels Responsible Entities to establish a risk-based methodology, including the procedures and

⁵ The IRC has grouped the various NOPR requests for comments by topic areas. As a result, the topical areas may not necessarily match the paragraph Order of the NOPR. The IRC has endeavored to detail the corresponding paragraph of the NOPR in these comments.

⁶ NOPR at P 115.

criteria that they used to develop their Critical Asset Lists. The IRC seeks clarification as to exactly what needs to be presented concerning the determination of which assets were left out of the definition of Critical Cyber Assets.

The IRC believes that inherent in any sound methodology for determining which assets represent Critical Cyber Assets is the determination of which assets should not be so categorized. In other words, if the methodology is thorough and well-documented, it should be clear how the determination was made as to which cyber assets are critical and which are not was made.

Furthermore, there are clear lines of corporate accountability established in the standard over these determinations. Reliability Standard CIP-003, Requirement R2 calls for entities to identify the Senior Manager who is accountable for leading the implementation and adherence to Reliability Standards CIP-002 through CIP-009. The identified Senior Manager is required by Reliability Standard CIP-002, Requirement R1 to approve the list of Critical Assets developed pursuant to the aforementioned risk-based methodology. Additionally, the modifications to the Reliability Standards proposed by the Commission in Paragraph 107 of the NOPR also compel the Senior Manager to explicitly approve the risk-based methodology used to develop the Critical Asset List. In the IRC's view, it is abundantly clear that the Senior Manager is fully accountable for both the thoroughness of the methodology used to establish the Critical Asset List as well as the completeness of the list itself.

If the Commission's intent was to ensure that the methodology for identification of Critical Cyber Assets makes clear why some assets were not so identified, then the proposal can and should be addressed by the ERO stakeholder process. However, if the

Commission intended a detailed asset by asset delineation of every asset not determined to be Critical Cyber Assets, the IRC respectfully submits that such a request may not be either workable or productive. In short, with a well-defined methodology, the determination of Critical Cyber Assets should be both clear and auditable. Any attempt to go further and require entities to “prove the negative” i.e. which assets were not so determined, could only work to cause confusion and provide unnecessary paperwork which will not enhance cyber security.

If the Commission deems that additional assurance of completeness is needed, the IRC recommends that compliance audits and/or NERC readiness reviews should include a process to periodically assess the thoroughness of the risk-based methodology and its application by Critical Asset owners. Accordingly, the IRC suggests that the Commission refrain from directing NERC to modify the Reliability Standards to require entities to detail, on an asset by asset basis those assets not determined to be Critical Cyber Assets. The Commission should instead clarify that it is simply requiring that the methodology that is being provided is sufficiently detailed such that it explains how different types of assets were determined to be either critical or non-critical.

B. Role of Demand Side Aggregators⁷

The IRC agrees with the Commission’s suggestion that “[d]emand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power system.”⁸

Demand-side aggregators are an increasingly important part of Bulk-Power System

⁷ The Alberta reliability framework outlined in Alberta legislation does not align well with the NERC Functional Model. The implementation of NERC-developed and FERC-approved reliability standards in Alberta (see footnote 1) will ensure alignment with Alberta legislation.

⁸ See NOPR at P 29.

operations and will continue to be relied upon more heavily for reliable and efficient operations.⁹ Even today, there may be demand-side aggregators that, through internet based communication systems, control large amounts of megawatts. It may be the case that not every demand-side aggregator needs to conduct the reviews and protections called for in the Reliability Standards or would even be considered “critical,” as the Standards are currently drafted, but the IRC agrees with the Commission’s suggestion that NERC needs to review whether such entities need to be included in the Compliance Registry. Adopting an approach of treating demand-side aggregators in comparable fashion with other users, owners and operators would be consistent with Order No. 890 as well.¹⁰

C. An Independent Determination of Critical Assets and Critical Cyber Assets

The Commission proposes in Paragraph 113 that there be a mechanism for the external review of Critical Asset lists based on a regional perspective. As the Commission observes: “If the vast majority of transmission owners, for example, identified a certain asset as critical, and a few did not, this result could be due to the unique circumstances of those transmission owners or from a flawed risk-based assessment methodology. However, without external oversight using a wide-area view,

⁹ See, e.g., EPAct of 2005, Section 1252(f) (“It is the policy of the United States that time-based pricing and other forms of demand response, whereby electricity customers are provided with electricity price signals and the ability to benefit by responding to them, shall be encouraged, the deployment of such technology and devices that enable electricity customers to participate in such pricing and demand response systems shall be facilitated, and unnecessary barriers to demand response participation in energy, capacity and ancillary service markets shall be eliminated.”).

¹⁰ See, e.g., Order No. 890 at P 888 (citing Staff Report: Assessment of Demand Response & Advanced Metering at 97-100 (Docket Number AD-06-2-000) (“Demand Response Report”)); see also *id.* at P 479 (“where demand resources are capable of providing the functions assessed in a transmission planning process, and can be relied upon on a long-term basis [citing Demand Response Report at 97-101], they should be permitted to participate in that process on a comparable basis. This is consistent with EPAct 2005 section 1223.”).

such trends or deviations would never be identified prior to an incident or audit, perhaps precluding a necessary adjustment to a particular critical asset list. In addition, a wide-area view would help to ensure that assets that have regional importance, such as for reactive power supply, are included as critical assets.”¹¹

At the same time, the Commission also observes that placing the responsibility for identifying Critical Assets on Regional Entities or another organization would “shift primary responsibility away from the asset owner or operator” and would “not improve the identification of critical assets.”¹² The IRC agrees. In that regard, the IRC offers the following comments for the Commission to consider in how the Standards may be improved.

Reliability Coordinators, not Regional Entities or Transmission Planners, should be the responsible entities to provide external oversight. This is because: (a) Regional Entities need to remain independent to enforce the Standards and should not be involved in Standard implementation, and (b) Transmission Planners are not sufficiently focused on the operational aspects of the grid where cyber security is most critical. .

Further, external organization (i.e., Reliability Coordinator)¹³ oversight should be limited to the methodologies for identifying “Critical Assets,” and not to “Critical Cyber Assets.” Reliability Coordinators have both a regional view that allows them to provide advice to asset owners so that there is coherence in how numerous, distinct asset owners identify Critical Assets and have the expertise in making such calls. By contrast, regulation of cyber assets is relatively new, and external organizations, such as Reliability

¹¹ NOPR at P 112.

¹² NOPR at P 111.

¹³ The Reliability Coordinator function in Alberta is facilitated through an agreement between the AESO and the Pacific Northwest Security Coordinator.

Coordinators (or Regional Entities for that matter), have no special expertise or insight in identifying methodologies for identifying Critical Cyber Assets.

In sum, the IRC agrees with the Commission that asset owners identify Critical Assets and that the perspective of an external organization, like a Reliability Coordinator which has a wide-area view that is focused on grid operations, can provide valuable oversight for the asset owner to take into account when it makes its determination.

D. Scope of Application (Market Data)

The argument that data is to be considered a critical cyber asset is first raised by the Commission in Paragraph 89 of the NOPR. In this paragraph, the Commission correctly notes that Cyber Assets are defined in the NERC Glossary as “programmable electronic devices and communication networks including hardware, software, and data,” and that Critical Cyber Assets are defined as “cyber assets essential to the reliable operation of critical assets.”¹⁴ However, Reliability Standard CIP-002-1, Requirement R3, in relevant part, further specifies that:

For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- R3.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- R3.2 The Cyber Asset uses a routable protocol within a control center; or,
- R3.3 The Cyber Asset is dial-up accessible.

The Commission further asserts that “marketing data or other data essential to the proper operation of a critical asset, and possibly the computer systems that produces or

¹⁴ NOPR at P 89.

process that data, would be considered Critical Cyber Assets subject to the CIP Reliability Standards.”¹⁵ On the strength of this assertion, the Commission proposes that it direct NERC to develop guidance regarding the steps necessary for applying the CIP Reliability Standards to the referenced data and to the computer systems that were used to produce the data.¹⁶

We submit that although the computers and other devices that contain data may use a routable protocol or may be dial-up accessible, the data itself does not use a routable protocol, nor is it, in its own right, dial-up accessible. Therefore, we submit that Reliability Standard CIP-002 does not require that “data” be considered a Critical Cyber Asset.

In addition, since every Responsible Entity’s definitive list of Critical Cyber Assets is developed pursuant to Reliability Standard CIP-002-1, Requirement R3, it is our view that the “further qualified” reference in Reliability Standard CIP-002-1, Requirement R3 applies to the use of the term “Critical Cyber Asset” wherever the term used in the Reliability Standards. Hence, it is our opinion that including data as a Critical Cyber Asset would go beyond the scope and intent of any of the Reliability Standards. This distinction is particularly important when one considers the impracticality of attempting to apply Requirements such as those in Reliability Standard CIP-003-1, Requirement R6 (change management and configuration control for changes to Critical Cyber Assets), and Reliability Standard CIP-007, Requirement R1 (testing of changes to Critical Cyber Assets) to data assets.

Finally, we respectfully suggest that the Commission may be in error in paragraph

¹⁵ NOPR at P 114.

¹⁶ *Id.*

114 of the NOPR where it concluded that “marketing or other data essential to the *proper* operation of a critical asset would be considered critical cyber assets subject to the CIP Reliability Standards.”¹⁷ [emphasis added] This conclusion appears to be based on an erroneous reference to the NERC Glossary definition of “Critical Cyber Assets” which refers to the “*reliable*” operation of Critical Assets. In that regard, while the “*proper*” operation of systems designed to control the power system may require that market systems used to improve economic efficiency should be operational, “*proper*” operation is not relevant in the context of the Reliability Standards. Rather, it is the *reliable* operation of an asset that is relevant (i.e., continuing to provide power when and where needed).

E. Scope of Application (Compliance with Corporate Policies)

The Commission notes in the NOPR that while some Requirements stipulate that a plan, policy, or procedure must be developed and maintained, simply doing so is not enough to satisfy the particular Requirement.¹⁸ Rather, the Commission states that it interprets the Requirement to include an implicit obligation to also “implement the plan, policy or procedure.”¹⁹ The Commission further opined that Responsible Entities should also be “subject to a non-compliance action for failing to implement the policy.”²⁰ We infer that the Commission also proposes to subject an entity to a non-compliance action for failing to implement a plan or procedure required by the Reliability Standards.

On its face, this proposal appears to be reasonable. We agree that merely producing a documented plan, policy, or procedure is not enough to satisfy any particular

¹⁷ NOPR at P 114.

¹⁸ NOPR at P 41.

¹⁹ *Id.*

²⁰ *Id.*

Requirement. Rather, the Reliability Standards require the production of these plans, policies, or procedures in order to attain some specific objective(s), and it is reasonable to require Responsible Entities to implement them to the extent necessary to meet those objectives. Thus, we request that NERC be directed to modify the Reliability Standards through the NERC standards development process to make this clear, preferably by clarifying the underlying objective of producing a plan, policy, or procedure.

Notwithstanding the foregoing, we are troubled by the Commission's expectation, expressed in paragraphs 126 and 127 of the NOPR, that Responsible Entities' security policies will address issues that are not currently reflected in the Reliability Standards.²¹ Taken in conjunction with the Commission's proposal to subject entities to a non-compliance action for failing to implement those policies, the IRC is concerned that entities could find themselves sanctioned although they are fully compliant with the specific Requirements of the Reliability Standards.

The IRC believes that the Commission should leave to a Responsible Entity's discretion, for reasons of efficiency or convenience, the decision whether to include within its "cyber security policy" certain provisions that go beyond those necessary to satisfy the Reliability Standards. The Responsible Entity may also draft its policy so that it is applicable to assets that are well beyond the scope of the Reliability Standards. However, failure to comply with portions of those policies that do not bear on the Reliability Standards is beyond the jurisdiction of NERC and the Regional Entity, and thus should not result in non-compliance actions. Responsible Entities should also be permitted to make exceptions to their internal policies where the exceptions have no bearing in the Reliability Standards, and they should be able to do so without the need to

²¹ NOPR at P 126 and P 127.

report them to any third party.

Accordingly, the IRC avers that if the Commission takes the position that failure to fully implement a corporate plan, policy or procedure will result in non-compliance, it will effectively drive entities toward developing multiple sets of plans, policies, and standards – those explicitly required by the Standards and those that may be applicable to other assets such as market systems. The IRC submits that compelling entities to develop separate sets of policies, plans and procedures would be inefficient, would result in greater overall costs, and may well be contrary to the Commission’s interests in ensuring efficient and effective operation of electricity markets. Thus, the IRC concludes that creating separate sets of policies and controls could result in the degradation of the overall effectiveness of organizational controls due to a potential possible lack of consistency inherent with a disparate or “stovepipe” control mechanism across an environment. Therefore, the IRC requests that the Commission clarify that monitoring for non-compliance shall be against the specific requirement of the Reliability Standards, not against requirements expressed in corporate policies which may be established to help entities address issues relevant to security.

F. Proving Functionality of Changes and Backups

The Commission notes that Reliability Standard CIP-003-1, Requirement R6 requires that Responsible Entities create “a process of change control and configuration management for adding, modifying, replacing, or removing critical cyber asset hardware or software.”²² The Commission proposes to include in this change control and configuration management process a requirement that “detection and monitoring controls” be utilized to ascertain whether changes have been made as they were intended

²² NOPR at P 140.

and to investigate whether any unplanned or unintended changes were made.²³ The IRC does not understand the Commission’s use of the phrase “detection and monitoring controls.” Hence, the IRC suggests to the Commission that it consider referring to “verification that unintended changes have not been made” rather than referring to “detection and monitoring controls” as relates to Reliability Standard CIP-003-1, Requirement R6.

What’s more, in cases where changes are manually initiated, we agree that it is appropriate to require entities to perform some sort of verification process to ensure that tested and approved hardware or software changes have been applied to the correct devices in the production environment. Along those lines, Responsible Entities should also be required to monitor their Critical Cyber Assets to determine whether unintended changes have been made to devices in the production environment, and to investigate and remediate instances where such unintended changes have been detected. If this is the full intent of the Commission’s proposed modifications to Reliability Standard CIP-003, Requirement R6, then the IRC is supportive.

However, the wording of the NOPR at paragraphs 144 and 148 suggests to the IRC that the Commission may expect entities to test the *functionality* of changes made to live, production systems to confirm that changes have been made as intended.²⁴ The IRC submits that it is not always possible to definitively, fully or safely confirm that applying a tested and approved change on a production device has necessarily had the same functional effect as that which was intended. This is particularly the case where the modification that is being intentionally introduced will be triggered only rarely under

²³ NOPR at P 144.

²⁴ See NOPR at P 144 and P 148.

specific operating conditions, or where testing on production systems could adversely affect power system reliability.²⁵ For better clarity, the IRC recommends that the Commission direct NERC to modify Reliability Standard CIP-003-1, Requirement R6 through the NERC standards development process to incorporate in the change control and configuration management process a requirement to verify that changes have been made on the intended devices, to monitor whether any unintended or unplanned changes have resulted, and to investigate and remediate any exceptions that are found to have occurred.²⁶

As a final point, there will be cases in which changes are intentionally initiated automatically using pre-approved means, such as automated virus signature updates and automated clock updates, for example. At times, these changes occur on an unpredictable schedule multiple times per day. We submit that it is impractical and unnecessary to verify each change as it happens. A requirement to do so is likely to result in entities choosing not to permit such automatic updates, which could easily have adverse reliability and security consequences.²⁷ Rather, the IRC believes that in such cases it would be appropriate to require that these Responsible Entities employ a program of *periodic* verification that the necessary updates, or their cumulative equivalent, have been effectuated. Of course, the IRC agrees that there remains a need to monitor for unintended or unauthorized changes even for automatically initiated changes.

G. Training Program Requirements

The Commission states that it intends to clarify that “cyber security training

²⁵ There are very real examples of such situations, however, the IRC believes it would be inappropriate to divulge them in a public document.

²⁶ *Id.*

²⁷ We are unable to provide specific examples herein due to the public nature of these comments.

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.”²⁸ The Commission further states 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.*”²⁹ [emphasis added] We respectfully disagree.

In that regard, the IRC concludes that except for some technical specialists (e.g., system administrators, network administrators, and security personnel), most personnel with access to Critical Cyber Assets are unlikely to need more than the most basic understanding of the specific “networking hardware and software and other issues of electronic interconnectivity supporting the operation” of those assets.³⁰ Furthermore, the IRC believes that it is imprudent to train staff on the vulnerabilities found in systems supporting Critical Cyber Assets unless that information is essential to the jobs they perform. In such a situation, training should focus on the proper operation of Critical Cyber Assets and on the behaviors and procedures necessary to avoid knowingly or unknowingly exploiting such vulnerabilities. The IRC asks the Commission to clarify that in all cases training should be appropriate for an employee’s duties, and should reveal information about technical provisions and vulnerabilities only on a “need to know” basis.

²⁸ NOPR at P 160.

²⁹ *Id.*

³⁰ *Id.*

H. Growth of Regional Entities

IRC members are concerned that several of the Commission's proposals will have the effect of placing significant additional burdens on NERC and/or the Regional Entities which are not justified by the benefits to be achieved. The result will be that Regional Entities will grow both in scope and size without any clear offsetting benefits. We are concerned that this growth would increase costs and create inefficiencies for Responsible Entities.

For instance, the Commission proposes, to direct NERC to develop a self-certification process that includes more frequent certifications, tied either to target dates in the schedule or to quarterly or semi-annual certifications.³¹ In the IRC's opinion, semi-annual certification would be far too frequent, and would require the expenditure of resources from Responsible Entities for the tracking and certification effort which are well beyond the benefits that would be generated. The IRC believes that a requirement for additional reporting will do little to speed up the compliance effort and would actually divert attention and resources away from important day-to-day tasks.

Furthermore, the Commission suggests that NERC and the Regional Entities work with Responsible Entities to assist in achieving compliance in a timely manner, including, if appropriate, the development of a remedial plan. The IRC does not believe that direct involvement of NERC or the Regional Entities in developing remedial plans is either: a. within their area of expertise or b. consistent with the need for appropriate separation between enforcement functions and advisory functions. Although the Commission's proposal on this subject appears benign, it could blur the need for separation of functions and cause unnecessary "mission creep" if not appropriately bounded. The IRC is

³¹ NOPR at P 48.

concerned that the charge to ERO may be read too broadly and does not reflect Commission recognition of the need for separation between the ERO and the Regional Entity serving as an enforcement arm vs. its becoming, in effect, a consultant to an individual registered entity assisting them in devising remediation plans. .

I. Approval of Exceptions by Third Parties

In the discussion of Technical Feasibility, the Commission notes its intention to “require a responsible entity to report and justify to the ERO and the Regional Entity for approval each exception and its expected duration.”³² The IRC submits that it is not appropriate to require Regional Entity approval of each “technical feasibility” exception that a registered entity might delineate. The IRC proposes an alternative construct for the Commission’s consideration.

First, the IRC does not believe that Regional Entities will have the expertise necessary to effectively assess “technical feasibility” on an entity by entity basis. This determination is not just a question of whether or not it is possible to do something; it is a question of whether or not it can be done using only the assets which exist at the moment at that particular Responsible Entity in light of their use of those assets in their business. Competently judging whether or not a proposed exception is justifiable on the grounds of “technical feasibility” would therefore require the Regional Entity to have full knowledge of, and considerable expertise in, every applicant’s specific circumstances. We believe this knowledge of every applicant to be unattainable given other responsibilities and designated tasks of the Regional Entity.

Second, we submit that granting the Regional Entities the authority to adjudicate exceptions while also granting them the ability to apply sanctions for non-compliance

³² NOPR at P 79.

places the Regional Entities in an untenable conflict of interest position. A fundamental tenet for auditors is independence; an assessor should not be involved with operational activities such as review and approval of policy exceptions.

Consequently, it is the IRC's view that the Regional Entities are not the appropriate parties to approve exceptions. Instead, the IRC poses the following alternative to address the need for a degree of consistency and oversight over individual entities invoking the "technical feasibility" exception. Specifically, the Commission should direct NERC to detail the type of justifications and considerations that must be documented as part of invoking the "technical feasibility exemption." Responsible Entities then must incorporate into their analysis the specific processes and "checklist" of determining factors that ERO has determined must be considered with specificity (and documented) prior to invoking the "technical feasibility" exemption. Further, giving NERC rather than the Regional Entities this responsibility will ensure that there is consistency in the requirements continent-wide. The Regional Entities' role should be limited to reviewing and determining whether a Responsible Entity has complied with these important but uniform exception process requirements.³³

J. Specification of How Requirements are to be Met

In the NOPR the Commission proposes that it direct NERC to modify the Reliability Standards to address the process for "how" requirements will be met.³⁴ The Commission also expressed concern that, "while NERC explains that the CIP Reliability

³³ It should also be noted that requiring Regional Entities or the ERO to undertake a detailed assessment of each entities' application of the technical feasibility exemption on an asset by asset basis will only increase competition for already scarce human resources. This is already a field of specialized expertise and efforts by ERO and the Regional Entities to employ people to meet this new requirement could frustrate efforts by registered entity's to employ these very same specialists.

³⁴ NOPR at P 33.

Standards are performance-based, the CIP Reliability Standards do not provide a mechanism to measure performance or otherwise determine whether a responsible entity has met the goals of a particular requirement set forth in the standards.”³⁵

The IRC supports the Commission’s proposed modifications to the CIP-002 requirements with regard to identifying Critical Assets and associated Critical Cyber Assets.³⁶ In that paragraph, the Commission indicates that improvement is needed in order to:

provide some basic guidance on the content or considerations to be applied in a risk assessment methodology. We are not proposing that NERC develop specific details of a methodology that must be applied in all circumstances. However, the Commission believes that responsible entities would benefit from NERC providing some common understanding regarding the scope, purpose and basic direction of the risk assessment methodology. For example, the Reliability Standard should indicate that a proper risk-based assessment methodology to identify critical assets should examine (1) **the consequences of the loss of the asset to the Bulk-Power System and (2) the consequence to the Bulk-Power System if an adversary gains control of the asset for intentional misuse**. Such guidance could also address how a generation owner, or even a partial owner of generation, without a wide-area reliability perspective, should approach a risk-based assessment. (emphases added)

The IRC supports the Commission’s suggestion because the Standard as currently drafted says little more than “do something.” As a practical matter, when possible, NERC in its drafting of standards should provide substantive guidance as to “what” is the reliability concern, so that companies can take corrective action, within their expertise, to do so. Without providing the substance of “what” is to be protected against, these Standards become nothing more than procedural exercises with little reliability benefit.

At the same time, however, the IRC believes that employing a standardized,

³⁵ NOPR at P 33.

³⁶ See NOPR at P 103.

system-wide approach to the details of implementation of each Reliability Standard would weaken overall security of the system, rather than strengthen it because an attacker would only have to find and exploit a single vulnerability on one system to be able to defeat the protection of like systems across the entire Bulk Electric system. This holds true for the act of identifying Critical Assets as well. Such standardization thus presents a significant risk in that potential intruders would easily be able to ascertain how systems are to be protected. With this information, they could easily refine attacks against those systems by working around the known controls, reducing the number of areas for which they must examine or investigate to determine the protective measures that may be present at all similar locations. Likewise, the Commission's comments elsewhere in the NOPR also apply here as well: "flexibility and discretion are essential in implementing the CIP Reliability Standards", and "Cyber security problems do not lend themselves to one-size-fits-all solutions."³⁷

Furthermore, if NERC or the Commission overly prescribe "how" compliance is to be achieved, there is a greater risk that protections taken to achieve compliance could quickly become obsolete. Given the explosion in the number of IT components, today's sound technical security solution may quickly be considered malpractice; whereas, Responsible Entities would be obligated to continue using outdated technologies and approaches until the Reliability Standard is revised. Accordingly, defining "what" needs to be done seems appropriate; however, describing "how" to do it would increase risk unnecessarily.

In view of the aforementioned concerns, the IRC concurs that a recommended approach to addressing the issue at hand would be to provide all affected parties with a

³⁷ NOPR at P 59.

clear description of the desired goal (i.e., “what” is required) rather than how to accomplish the goal). Clear objectives would not only give an entity a clear understanding of when they have achieved compliance, but they will also facilitate the evaluation process itself. Providing clear, concise, objective statements to entities will give them adequate guidance without unnecessarily limiting their approach to achieving the objective. Therefore, we ask the Commission not to require the inclusion of “how” language within the Reliability Standards. Rather, NERC should be permitted to prepare external guidance documents that incorporate this information, but such guidance should not be contained in the Reliability Standards.

K. Contractual Obligations for Outsourced Functions

Finally, in the NOPR, the Commission invites comment on how key functions may be outsourced and whether third-party entities should be contractually obligated to comply with the Reliability Standards while satisfying their other contractual obligations to a Responsible Entity, Regional Entity or NERC, and how this all may be accomplished.³⁸

In that regard, the IRC concurs with the Commission “that access to information essential to the operation of critical cyber assets by out-sourced entities that are not otherwise subject to the CIP Reliability Standards presents a potential vulnerability to the Bulk-Power System.”³⁹ Further, it is the opinion of the IRC that security should be embedded within applications. Thus, if an application is essential to the reliable operation of the bulk electric system, it is a critical cyber asset. Moreover, when an application is developed and maintained by an outsourced provider, that outsourced

³⁸ NOPR at P 31.

³⁹ *Id.*

provider manages physical and cyber access to the environment on which the application runs and therefore must be contractually obligated by the Responsible Entity to comply with the Reliability Standards.

While such providers are not registered entities subject to the Reliability Standards, they must perform the services and operate the applications in a manner consistent with the Reliability Standards. Although it is neither practical nor appropriate to hold third parties responsible for compliance with the Reliability Standards in the usual manner, the Responsible Entity should be charged with incorporating contractual terms and conditions into its agreements with third-party service providers that obligate the providers to comply with the requirements of the Reliability Standards. In that regard, if a Responsible Entity determines that it is necessary to outsource a service that is essential to the reliable operation of a Critical Asset, Critical Cyber Asset or the Bulk Electric system, it is clear that the Responsible Entity must be held responsible and accountable for compliance with the Reliability Standards. Consequently, any penalties or sanctions resulting from the third-party's failure to comply with the Reliability Standards should be borne by the Responsible Entity that made the business decision to outsource the key service or application. However, this should not preclude Responsible Entities from including terms and conditions in their agreements with third-party providers that bind the service provider to the requirements of the Reliability Standards and which allow for reimbursement of any penalties or sanctions imposed, or damages resulting, from non-compliance with the Reliability Standards.

For existing services, contract negotiations with providers may begin at any time. However, requirements from the Reliability Standards must be included as appropriate

for agreements that take effect no later than the first contract renewal following Commission approval of the Reliability Standards. For new services, a third party provider must be obligated to comply with the Reliability Standards at the inception of the contract.

If an existing outsourced provider refuses to be contractually bound to the requirements of the Reliability Standards, the Responsible Entity should be afforded a reasonable period of time to seek another, more willing provider, or bring the services in-house. Failure to do either should result in a finding of non-compliance in the absence of an independent audit, with the Responsible Entity bearing the full brunt of the applicable penalties.

The Responsible Entity has the obligation to demonstrate that the outsourced provider is compliant with the requirements of the standards. This may be documented by a triennial audit conducted by an independent party and self-certification by the provider in the intervening years.

Some providers may perform similar out-sourced services to a large number of Electric Sector entities. The provider should be afforded the option to voluntarily comply with the requirements of the Reliability Standards and submit themselves to the formal audit processes of the Regional Entity whose footprint encompasses the location where the out-sourced services are performed. An audit by the Regional Entity would be binding upon all entities for which services are provided. Consideration should be given in the final order to allow the out-sourced provider to voluntarily submit to any financial sanctions resulting from the audit. Such an agreement would absolve Responsible Entities from additional sanctions and would allow the services provider to avoid the risk

of multiple financial penalties for the same violation.

III. CONCLUSION

For the reasons set forth above the IRC respectfully requests that the Commission adopt the IRC recommendations set forth above and expeditiously issue a final rule in this proceeding.

Respectfully submitted,

/s/ Craig Glazer

Craig Glazer
Vice President – Federal Government
Policy
Jacquelyn B. Hugee – Senior Counsel
Steven R. Pincus – Senior Counsel
PJM Interconnection, L.L.C.
1200 G Street, NW, Suite 600
Washington, DC 20005

/s/ Stephen G. Kozey

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

/s/ Theodore J. Paradise

Theodore J. Paradise
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, MA 01040

/s/ Anthony J. Ivancovich

Nancy Saracino
Vice President, General Counsel &
Corporate Secretary
Anthony J. Ivancovich
Assistant General Counsel
**California Independent System
Operator Corporation**
151 Blue Ravine Road
Folsom, CA 95630

/s/ Kim Warren

Kim Warren
Manager, Regulatory Affairs
**Independent Electricity System
Operator of Ontario**
655 Bay Street, Suite 410
Toronto, Ontario M5G-2K4

Robert E. 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 Pommen
Director Interjurisdictional Affairs
**Independent System Operator operating
as the Alberta Electric System Operator**
Calgary Place
2500 330 - 5th Avenue SW
Calgary, AB T2P 0L4

/s/ Stacy Duckett

Stacy Duckett
General Counsel & Corporate Secretary
Southwest Power Pool
415 North McKinley
#140, Plaza West
Little Rock, AR 72205-3020

/s/ Michael G. Grable

Michael G. Grable
Assistant General Counsel
Electric Reliability Council of Texas
7620 Metro Center Drive
Austin, TX 78744

October 5, 2007