

RSSC Members:

Per discussions at the recently concluded RSSC meeting, attached are the draft comments of the ISO-RTO Council regarding the FERC Notice of Proposed Ruling (NOPR) on the Critical Infrastructure Protection (CIP) standards. Please review the attached document and let us know if there are any concerns or if additional information is required. These comments, once firmed up, will be filed by the council with FERC, on October 5<sup>th</sup>.

About the ISO-RTO Council:

Founded in 2003, the ISO/RTO Council (IRC) is an industry organization comprised of 10 Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) in North America. These ISOs and RTOs deliver two-thirds of the electricity consumed in North America to two-thirds of its population. Additional information on the council can be obtained at: <http://www.isorto.org>

On July 20, 2007, the Federal Energy Regulatory Commission issued a Notice of Proposed Rulemaking [Docket No. RM06-22-000] which proposes certain courses of action regarding the eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC).

The ISO/RTO Council, which represents the 10 Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) in North America, respectfully submits the following comments on FERC's proposed rulemaking.

The ISO/RTO council commends FERC and its staff for the thoughtful assessment of the NERC CIP Standards which underscores the NOPR. We believe that FERC's proposal to approve all eight Standards and their proposal to approve NERC's Implementation Plan and associated timelines for achieving compliance are important steps towards ensuring that Responsible Entities have taken necessary precautions against events which could jeopardize Bulk Electric System reliability.

While we strongly support this overall theme of the Commission's proposals, there are some details of the Commission's comments and proposals which concern us and upon which we would like to comment. In our discussion below, we present our concerns in the following topical areas:

- (1) Critical Asset determination
- (2) Scope of Application (Market Data)
- (3) Scope of Application (Compliance with Corporate Policies)
- (4) Revocation of Access to Information
- (5) Revocation of Access to Critical Cyber Assets
- (6) Proving Functionality of Changes and Backups
- (7) Training Program Requirements
- (8) Growth of Regional Entities
- (9) Approval of Exceptions by Third Parties
- (10) Specification of How Requirements are to be Met
- (11) Contractual Obligations for Outsourced Functions

## 1. Critical Asset Determination

In Paragraph 115 the Commission proposes to require that entities show why specific assets were or were not chosen as critical assets. In our opinion, this should not be necessary.

CIP-002 R1 already requires entities to establish a risk-based methodology, including procedures and criteria used to develop their Critical Asset Lists. CIP-003 R2 requires entities to identify the Senior Manager with accountability for leading the implementation and adherence to CIP-002 through CIP-009. That manager is required by CIP-002 R1 to approve the list of Critical Assets developed pursuant to the aforementioned risk-based methodology. With the modifications to the Standards proposed by the Commission in Paragraph 107, the Senior Manager will also be required to explicitly approve the risk-based methodology used to develop

the Critical Asset List. In our view, this makes it abundantly clear that the Senior Manager is fully accountable for both the thoroughness of the methodology used to establish the Critical Asset List and the completeness of the list itself. We submit that requiring documentation of why various assets were *not* determined to be critical assets is an unnecessary burden. If additional assurance of completeness is needed, we recommend 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.

## **2. Scope of Application (Market Data)**

In Paragraph 114 of the NOPR, the Commission asserts that “marketing data 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 a critical cyber asset subject to the reliability Standards”. On the strength of this assertion, 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 which produce the 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 Critical Cyber Assets are defined [in the NERC Glossary] as “programmable electronic devices and communication networks including hardware, software, and data.” However, CIP-002-1 R3 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”.

We submit that data does not use a routable protocol, nor is it, in its own right, dial-up accessible. Granted, the devices which contain data may use a routable protocol or be dial-up accessible, but not the data itself. Hence, we submit that CIP-002 does not require data to be considered a Critical Cyber Asset

Since every Responsible Entity’s definitive list of Critical Cyber Assets is developed pursuant to CIP-002-1 R3, it is also our view that the “further qualification” quoted above for the purpose of Standard CIP-002 applies to the use of the term “Critical Cyber Asset” wherever the term used in the CIP Standards. Hence, it is our submission that including data as a Critical Cyber Asset would go beyond the scope of any of the CIP Reliability Standards.

In further support of this view, members of the NERC Cyber Security Standards Drafting Team who were involved with developing the Standard and defining the term “Critical Cyber Asset” have confirmed that the term “data” was intended to refer to information *about* the Critical Cyber

Asset, not to information being processed *by* the Asset. This distinction is particularly important when one considers the impracticality of attempting to apply Requirements such as those in CIP-003-1 R6 (change management and configuration control for changes to Critical Cyber Assets), and CIP-007 R1 (testing of changes to Critical Cyber Assets) to data assets.

We further respectfully suggest that the Commission may be in error in paragraph 114 of the NOPR where it is 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.” [emphasis added]. This conclusion appears to be based on an erroneous reference to the NERC Glossary definition of critical cyber assets. We note that the definition of “Critical Cyber Assets” refers to the *reliable* operation of critical assets, not to the *proper* operation. While *proper* operation of systems designed to control the power system may require that market systems used to improve economic efficiency should be operational, it is not *proper* operation which is relevant in the context of the CIP standards. It is *reliable* operation that is relevant (i.e., continuing to provide power when and where needed).

### **3. Scope of Application (Compliance with Corporate Policies)**

In paragraph 41 the Commission notes that while some Requirements stipulate that a plan, policy, or procedure must be developed, simply doing so is not enough. The Commission states that it “interprets such provisions to include an implicit requirement to implement the plan, policy or procedure”. It is further proposed to “make a responsible entity subject to a non-compliance action for failing to implement the policy”. 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 Standards.

On the face of it, this seems reasonable. We agree that merely producing a documented plan, policy, or procedure is not enough. The Standards require the production of these plans, policies, or procedures in order to attain some specific objective or objectives, and it is reasonable to require Responsible Entities to implement them to the extent necessary to meet those objectives. The ERO should be directed to modify the Standards to make this clear, preferably by clarifying the underlying objective of producing a plan, policy, or procedure.

However, we are troubled by the Commission’s expectation, expressed in paragraphs 126 and 127, that responsible entities’ security policies will address issues that are not currently reflected in the CIP Reliability Standards. Taken in conjunction with the Commission’s proposal to subject entities to non-compliance action for failing to implement those policies, we are concerned that entities could find themselves sanctioned even though they are fully compliant with the specific Requirements of the CIP Reliability Standards.

A Responsible Entity may choose for reasons of efficiency or convenience to include within its “cyber security policy” certain provisions that go beyond those necessary to satisfy the CIP Standards. It may also draft that policy so that it is applicable to assets that are well beyond the scope of the CIP standards. Failure to comply with portions of those policies that do not bear on

the CIP Reliability Standards is beyond the jurisdiction of the ERO and the Regional Entity, and should not attract non-compliance actions. By corollary, entities should be able to take exceptions to their internal policies where that has no bearing in the CIP Reliability Standards, and they should be able to do so without the need to report them to any third party. .

Should the Commission take the position that failure to fully implement a corporate plan, policy, or procedure will result in non-compliance, we suggest 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. We submit that driving entities to develop separate sets of policies, plans and procedures would be inefficient, will result in greater overall costs, and may well be contrary to the Commission’s interests in ensuring efficient and effective operation of electricity markets. Separate sets of policies and controls also have the potential to degrade the overall effectiveness of organizational controls due to a possible lack of consistency inherent with disparate or “stovepipe” control mechanism across an environment.

#### **4. Revocation of Access to Information**

In paragraph 139, the Commission discusses the importance of revoking access to information. While this is a very valid comment, from a technological perspective, revoking access to protected information and not just physical or logical access is not feasible. The only way to accomplish this is to manage all protected information, both electronic and physical, by tracking its transmission and handling. This involves much more than just data encryption or classification and extends beyond digital rights management to tangible hard copy information. This is technically not feasible for information in hard copy or in the possession or knowledge of individuals. In addition, all protected logical information, electronic documents and emails would require information tracking TTL (time to live) designation and control on copying, editing or forwarding. The best way to handle the revocation of access to information is to have strong procedural controls in place for when someone with access to critical data no longer needs such access.

#### **5. Revocation of Access to Critical Cyber Assets**

In Paragraph 169, the Commission 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 for any reason”. The Commission further asserts that this will not be unduly burdensome for Entities. While we agree that rapid revocation of access privileges is essential in exigent circumstances where a termination or transfer might be deemed “unfriendly” (e.g., “for cause”), we submit that “immediate revocation” is an inordinately stringent requirement in cases of voluntary staff transfer within the same Entity.

Firstly, we suggest that there is an inherent difficulty in requiring “immediate” revocation. Revoking access is not an instantaneous process since it is almost always necessary to revoke

privileges on multiple systems. Termination of physical, and network (including remote access) access can generally be accomplished relatively quickly and easily, but revocation of subordinate accounts and services often requires considerably more effort. Furthermore, it is sometimes necessary that subordinate accounts not be disabled or removed to facilitate management purposes such as the maintenance of records and audit trails.

We also submit that there is a very low risk that a staff member who had legitimate access to Critical Cyber Assets immediately before a voluntary job transfer will use his/her access permissions maliciously or carelessly shortly after the transfer occurs. Building and maintaining a highly reliable business process to ensure “immediate” revocation in such instances will only serve to increase costs with minimal risk reduction.

Finally, the requirement to immediately revoke access when a job function is no longer performed does not appear to contemplate that staff may transfer out of a specific job function (thus not perform the function any longer), but may continue to be relied on to provide backup when the nominal incumbent is unavailable. We suggest that the ERO should be instructed to accommodate this consideration when the Standard is revised.

## **6. Proving Functionality of Changes and Backups**

In Paragraph 141, the Commission proposes to “include in the process of change control and configuration management a requirement for detection and monitoring controls to determine if changes are made as intended and to investigate whether any unintended or unplanned changes have been made”.

We find the use of the phrase, “detection and monitoring controls” confusing, and suggest that the Commission might consider referring to “verification that unintended changes have not been made” rather than referring to “detection and monitoring controls”.

In cases where changes are manually initiated, we agree that it is appropriate to require entities to perform some sort of verification to ensure tested and approved hardware or software changes have been applied to the correct devices in the production environment. Entities should also be required to monitor to determine whether unintended changes have been made to devices in the production environment, and to investigate and remediate instances where this is detected. If this is the full intent of the Commission’s proposed modifications to CIP-003 R6, then we are in agreement.

However, the wording used in the NOPR at paragraph 144 and again in paragraph 148 suggests 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. We submit that it is sometimes not possible to definitively and 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 specific operating conditions, or where testing on production systems could adversely affect power system reliability. For better

clarity, we recommend that the Commission should direct the ERO to modify Requirement R6 of Reliability Standard CIP-003-1 to “include in the process of change control and configuration management a requirement to verify that changes are made on the intended devices, to monitor for unintended or unplanned changes, and to investigate and remediate any exceptions that are found”.

There will be cases where changes are intentionally initiated automatically using pre-approved means (e.g., automated virus signature updates, automated clock updates, etc). Sometimes, 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. Rather, we submit that in such cases it would be appropriate to require that there is a program of *periodic* verification that the necessary updates, or their cumulative equivalent, have been done. Of course, even for automatically initiated changes, there remains a need to monitor for unintended or unauthorized changes.

## **7. Training Program Requirements**

In paragraph 160 the Commission states that it intends to clarify that “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”. Later in Paragraph 160, the Commission 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.*” [emphasis added] . We respectfully disagree.

We submit 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. We further submit that it is most unwise to train staff on the vulnerabilities found in systems supporting Critical Cyber Assets unless that information is essential to the jobs they perform. 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. 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.

## **8. Growth of Regional Entities**

We are concerned that several of the Commission’s proposals will have the effect of placing significant additional burdens on the ERO and/or the Regional Entities. The result will be that Regional Entities will grow both in scope and size. We are concerned that this will increase costs and create inefficiencies.

In Paragraph 48, for instance, the Commission 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”. In our 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. We believe 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 the ERO and the Regional Entities should work with Responsible Entities to assist in achieving compliance in a timely manner, including, “if appropriate” the development of a remedial plan. This will add considerable strain to both NERC and Regional Entity resources, and will result in increased costs for these organizations and ultimately for the industry as a whole. This is not justified, particularly as Entities have sufficient incentive to comply with the overall timeline by virtue of being subject to substantial financial penalties and sanctions if they are found they are found to be non-compliant.

### **9. Approval of Exceptions by Third Parties**

In the text of Para 79, 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.” It is unclear whether the Commission intends that both the ERO and the Regional Entity approve exceptions, or whether it is just the Regional Entity. We submit that requiring review and approval by both entities would not provide any substantial benefit.

Furthermore, we submit that it is not appropriate to require approval of proposed exceptions by the Regional Entity, or by any other third party for that matter. In our comments below we focus on the difficulties posed by requiring Regional Entities to approve exception requests, but analogous arguments lead us to believe that approval by any third party is inappropriate. We have comments in the following areas:

- (a) dilution of responsibility
- (b) necessary expertise
- (c) concentration of information
- (d) competition for key technical staff resources
- (e) focus on adversarial process
- (f) approval delay
- (g) conflict of interest
- (h) stakeholder interests

### **Dilution of Responsibility**

First, we note that the Commission stated in paragraph 111 that the responsibility for identifying and approving lists of critical assets should not be placed on the Regional Entities or another organization other than the Responsible Entities. In the Commission’s words, “Such an

approach would shift primary responsibility away from the asset owner or operator. We believe that such a shift would not improve the identification of critical assets, but more likely overwhelm the Regional Entities.” In our view, requiring exceptions to be reviewed and approved by the Regional Entity is an analogous situation. Requiring approval of exceptions by other than the entities concerned would tend to dilute responsibility for properly assessing technical feasibility. The Regional Entity will quickly become overwhelmed by the need to carefully assess exception requests, particularly if, as per paragraph 191, the Commission intends to require Regional Entities to perform detailed technical reviews of “the application of ‘technical feasibility’ as the basis for allowing a responsible entity an exception to full compliance with a Requirement.”

We submit that properly identifying and approving exceptions based on technical feasibility is no more critical to the thorough implementation of the CIP standards than is the initial identification and approval of lists of critical assets. The Commission has quite rightly noted that responsibility for the latter must rest squarely with the Responsible Entities. So should the former. Approval by the Regional Entity should not be required.

### **Necessary Expertise**

We also question whether Regional Entities will have the expertise necessary to assess technical feasibility. Under the Commission’s proposal in paragraph 77 of the NOPR, technical feasibility would be interpreted “narrowly as applying to the technical characteristics of *existing assets*” (emphasis added). Hence, “technical feasibility” 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. 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 to be unattainable given other Regional Entity responsibilities and designated tasks.

### **Concentration of Information**

Furthermore, to competently judge the validity of an exception request, Regional Entity staff would need access to a considerable body of highly sensitive information about each entity. The Regional Entity would quickly develop a large repository of information about critical cyber assets, their vulnerabilities, and how to exploit them – essentially a guidebook on how to compromise the entire bulk power system. We submit that concentrating such information at the Regional Entities poses far too high of a risk for compromise, either through accident, carelessness, or successful malicious attack.

### **Competition for Key Technical Staff Resources**

Of course, if Regional Entities are placed in the position where they are obliged to pass judgement on the technical feasibility of exception requests, they will undoubtedly seek to manage the attendant expectations and liabilities by hiring competent key technical staff. This will force increased competition for already scarce human resources. This will inevitably

increase costs that have to be recovered from ratepayers. It is also likely that the overall security posture of the industry will suffer, at least in the short term, as resources are drawn away from dealing with real, “on the ground” security matters and are moved towards management of exceptions and relationships between Regional Entities and Responsible Entities.

### **Focus on Adversarial Process**

We submit that requiring approval of exceptions by Regional Entities or other third parties will result in sub-optimal allocation of those scarce, technically competent staff resources. We suggest that Responsible Entities are likely to focus increased resources on the process of seeking exceptions with fewer resources available to address the underlying circumstance that gives rise to the exception. Entities will tend to focus on “making their case”. Litigation can be anticipated when exception requests are denied, and Regional Entities will likely develop new mechanisms, such as appeals processes, to help manage the liabilities attendant with their new role as adjudicators. Bureaucratic engines will result, both within the Responsible Entities and within the Regional Entities. Considerable effort will be expended with no substantive improvement in power system reliability.

### **Approval Delay**

We are also concerned that Regional Entities may find themselves overwhelmed by exception requests to the point where their staff are unable to process the requests in a timely manner. This is particularly likely as key dates for compliance approach. If the Commission insists that Regional Entities or any other third parties are to approve all requests for exceptions on the grounds of technical feasibility, we urge that they also carefully consider, and appropriately direct the ERO to clarify how Regional Entities and Responsible Entities are to treat situations in which a request for an exception either has not been adjudicated, is currently under appeal, or has been adjudicated with insufficient time for a Responsible Entity to respond.

### **Conflict of Interest**

Finally, we submit that granting the Regional Entities the authority to adjudicate exceptions while also granting them the ability to apply sanctions for non-compliance places the Regional Entities in an untenable conflict of interest position. Claims of conflict will arise when exceptions are denied, non-compliance is subsequently determined, and financial sanctions are applied.

To reiterate, we submit that it would be inappropriate to modify the standards to require that exceptions should be approved by the Regional Entities, or by any other third party. We submit that review of exception requests by the Responsible Entity’s “senior manager” with acceptance and formal sign-off only on the grounds of technical infeasibility, combined with a program of periodic audits of the rationales provided and the stiff financial sanctions for non-compliance that are already contemplated in the Standards will provide more than enough assurance that exceptions will not be approved inappropriately.

## **10. Specification of How Requirements are to be Met**

In paragraph 33 of the NOPR, the Commission proposes to direct NERC to modify the CIP Reliability Standards to address “how” requirements will be met. The Commission also expressed their concern that, “while NERC explains that the CIP Reliability 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.”

We are concerned that a standardized, system-wide approach to implement each CIP Standard would weaken overall security, rather than strengthen it. Defining “what” needs to be done seems appropriate; however, describing “how” to do it would unnecessarily increase risk.

With a standardized approach to address each CIP Standard, 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 presents a significant risk in that potential intruders would easily be able to know 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 where they must “guess at” the protective measures that may be present at all similar location.

Another risk is that today’s “how” could quickly become obsolete tomorrow. 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 CIP Standard is revised.

The Commission’s comments in paragraph 59 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.”

A recommended approach would be a clear description of the desired goal (i.e., “what” is required, not how to do it). Clear objectives would not only help an entity know when they have achieved compliance, but would also facilitate the evaluation process itself.

Clear, concise, objective statements would provide adequate guidance to entities without unnecessarily limiting their approach to achieving it. One example of this approach is the requirement for performing reviews of electronic access points to the electronic security perimeter (ESP).

## **11. Contractual Obligations for Outsourced Functions**

In Paragraphs 31 of 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 CIP Reliability Standards while satisfying their other contractual obligations to a Responsible Entity, Regional Entity or the ERO.

We concur 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.”

Security should be embedded within applications. If an application is essential to the reliable operation of the bulk electric system, it is a critical cyber asset. When an application is developed and maintained by an outsourced provider, they manage physical and cyber access to the environment where the application runs and must be contractually obligated by the Responsible Entity to comply with the NERC CIP Reliability Standards.

While such providers are not registered entities subject to the CIP Standards, they must perform the services and operate the applications in a manner consistent with the CIP Standards. Since it is neither practical nor appropriate to hold third parties responsible for compliance to the CIP Standards in the usual manner, the Responsible Entity is responsible for including contractual terms and conditions that bind third-party service providers to comply with the requirements of the CIP Reliability Standards.

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, the Responsible Entity must be held responsible and accountable for compliance. Any penalties or sanctions resulting from the third-party’s failure to comply with the NERC CIP Reliability Standards should be borne by the Responsible Entity that decided to outsource the key service or application. This should not preclude Responsible Entities from including contractual terms and conditions in their agreements with third-party providers that would bind the service provider to the requirements of the CIP Reliability Standards and allow for reimbursement of any penalties or sanctions, or damages resulting from non-compliance with the CIP Reliability Standards.

For existing services, contract negotiations with providers may begin at any time. However, requirements from the CIP Standards must be included as appropriate for agreements that take effect no later than the first contract renewal following FERC approval of the NERC CIP Reliability Standards.

For new services, a provider must be obligated with the initial term of the contract.

If an existing outsourced provider refuses to be contractually bound to the requirements of the CIP 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 penalties.

The entity has the obligation to demonstrate 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 CIP 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.

DRAFT