

Standards Development
Guideline Development
ERO Staff/Process
Items of Note

Order 706

Commission Determination Statements

24. The Commission approves the eight CIP Reliability Standards pursuant to section 215(d) of the FPA, as discussed below. In approving the CIP Reliability Standards, the Commission concludes that they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. These CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support the nation's Bulk-Power System. Thus, the CIP Reliability Standards serve an important reliability goal. Further, as discussed below, the CIP Reliability Standards clearly identify the entities to which they apply, apply throughout the interconnected Bulk-Power System, and provide a reasonable timetable for implementation.

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

26. With regard to WIRAB's recommendation, we share the ongoing concern of promoting coordinated action on Reliability Standards on an international basis. However, in this instance, we do not believe a remand to NERC, which would result in significant delays in having mandatory and enforceable cyber security requirements in effect in the United States, is justified or would further such coordination. The implementation schedule provided by NERC, which applies continent-wide, requires applicable entities to achieve "auditable compliance" no earlier than mid-2009. This should provide adequate time for entities responsible for compliance with the CIP Reliability Standards in the United States, Canada and Mexico to achieve compliance on a common timetable. As discussed later, future modifications to the CIP Reliability Standards developed pursuant to the direction provided in the Final Rule would not overlap with the NERC implementation plan. Accordingly, the Commission concludes that this is not a satisfactory reason for remanding the CIP Reliability Standards.

27. In approving the CIP Reliability Standards and directing the ERO to modify them, the Commission is taking two independent actions and does not condition our approval on the ERO modifying the CIP Reliability Standards. First, we are exercising our authority to approve a proposed Reliability Standard. Second, we are directing the ERO to submit a modification of the Reliability Standards to address specific issues or concerns. Accordingly, New York Commission's concerns about the Commission placing any conditions on its approval of the CIP Reliability Standards are unnecessary.

28. With regard to the concerns raised by some commenters about the prescriptive nature of the Commission's proposed modifications, the Commission agrees that a direction for modification should not be so overly prescriptive as to preclude the consideration of viable alternatives in the ERO's Reliability Standards development process. However, in identifying a specific matter to be addressed in a modification to a CIP Reliability Standard, it is important that the Commission provide sufficient guidance so that the ERO has an understanding of the Commission's concerns and an appropriate, but not necessarily exclusive, outcome to address those concerns. Without such direction and guidance, a Commission proposal to modify a CIP Reliability Standard might be so vague that the ERO would not know how to adequately respond.

29. Thus, in some instances, while we provide specific details regarding the Commission's expectations, we intend by doing so to provide useful guidance to assist in the Reliability Standards development process, not to impede it. We find that this is consistent with statutory language that authorizes the Commission to order the ERO to submit a modification "that addresses a specific matter" if the Commission considers it appropriate to carry out section 215 of the FPA. In the Final Rule, we have considered commenters' concerns and, where a directive for modification appears to be determinative of the outcome, the Commission provides flexibility by directing the ERO to address the underlying issue through the Reliability Standards development process without mandating a specific change to the CIP Reliability Standard. Further, the Commission clarifies that, where the Final Rule identifies a concern and offers a specific approach to address that concern, we will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will adequately address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal.

30. Consistent with section 215 of the FPA, our regulations, and Order No. 693, any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and fully vetted through NERC's Reliability Standard development process. Until the Commission approves NERC's proposed modification to a Reliability Standard, the preexisting Reliability Standard will remain in effect.

47. The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards. The Commission maintains its belief that NERC's compliance is necessary in light of its interconnectivity with other entities that own and operate critical assets. Further, we conclude that NERC's Rules of Procedure, which state that the ERO will comply with each Reliability Standard that identifies the ERO as an applicable entity, provides an adequate means to assure that NERC is obligated to comply with the CIP Reliability Standards. Likewise, the delegation agreements between NERC and each Regional Entity expressly state that the Regional Entity is committed to comply with approved Reliability Standards. Based on these provisions, we find that the Commission has authority to oversee the compliance of NERC and the Regional Entities with the CIP Reliability Standards.

48. With regard to EEI's concerns about NERC's incentives to comply with the CIP Reliability Standards, we believe that NERC's position as overseer of Bulk-Power System reliability provides a level of assurance that it will take compliance seriously. Moreover, section 215(e)(5) of the FPA provides that the Commission may take such action as is necessary or appropriate against the ERO or a regional entity to ensure compliance with a Reliability Standard or Commission order.

49. The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards. We are concerned, like the California Commission, that some small entities that are not identified in the NERC registry may become gateways for cyber attacks. However, we are not prepared to adopt California Commission's suggested approach of requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry. We believe this approach is overly-expansive and may raise jurisdictional issues. Rather, we rely on NERC and the Regional Entities to be vigilant in assuring that all appropriate entities are registered to ensure the security of the Bulk-Power System.

50. With regard to EEI's request for clarification, the NERC registry process is designed to identify and register entities for compliance with Reliability Standards, and not identify lists of assets. In the CIP NOPR, the Commission explained that it would expect NERC to register the owner or operator of an important asset, such as a blackstart unit, even though the facility may be relatively small or connected at

low voltage. While the facility would not be registered or listed through the registration process, NERC's or a Regional Entity's awareness of the critical asset may reasonably result in the registration of the owner or operator of the facility.

51. Likewise, **we believe that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.** EEI and ISO/RTO Council concur that the need for the registration of demand side aggregators may arise, but state that it is not clear whether aggregators fit any of the current registration categories defined by NERC. **We agree with EEI and ISO/RTO Council that NERC should consider whether there is a current need to register demand side aggregators and, if so, to address any related issues and develop criteria for their registration.**

52. The Commission agrees with the many commenters that suggest that **the responsibility of a third-party vendor for compliance with the CIP Reliability Standards is a matter that should be addressed in contracts between the registered entity that is responsible for mandatory compliance with the Standards and its vendor.** To the extent that the responsible entity makes a business decision to hire an outside contractor to perform services for it, **the responsible entity remains responsible for compliance** with the relevant Reliability Standards. Thus, it is incumbent upon the responsible entity to assure that its third-party vendor acts in compliance with the CIP Reliability Standards. We agree with ISO/RTO Council's characterization of the matter:

. . . when an application is developed and maintained by an outsourced provider, that outsourced provider manages physical and cyber access to the environment on which the application runs and therefore must be contractually obligated to 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. . . the Responsible Entity should be charged with incorporating contractual terms and conditions into 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.

53. Further, it is incumbent upon a responsible entity to **conduct vigorous oversight of the activities and procedures followed by the vendors they employ. Thus, we expect a responsible entity to address in its security policy under CIP-003-1 its policies regarding its oversight of third-party vendors.**

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to **implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result.** Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, **in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require that the guidance be placed in modifications to the CIP Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.**

62. Some of the more specific directives in this Final Rule pertain to issues that the Commission considers necessary to carry out its statutory responsibilities. **Examples of this include areas of oversight, exceptions to Requirements, and reports to the Commission.** In developing these directives, we have tried to strike a balance between our needs to implement the statute and the concerns expressed by commenters.

63. We agree in general with commenters who point out that compliance issues should be determined in audits and that a strong auditing process will help to ensure quality control and consistency in the implementation of the CIP Reliability Standards. However, **we point out that audits are only one aspect of the ERO's compliance monitoring and enforcement process.** All aspects of that process must function well. In addition, we note compliance audits are conducted after-the-fact and do not diminish the **necessity for internal and external reviews of compliance efforts, including the identification of critical assets and critical cyber assets.**

64. In response to Northern Indiana, we explain “external oversight” in our discussions and determinations of specific Requirements in the Final Rule.

72. While the Commission agrees with commenters that relying on an objective determination such as whether a document exists would facilitate the compliance audit process, we do not believe such a cursory approach is the best way to ensure the protection of the Bulk-Power System. **We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement.** In this way we **affirm the Commission's position established in Order No. 693** that, “while Measures and Levels of Non-Compliance provide useful guidance to the industry, compliance will in all cases be measured by determining whether a party met or failed to meet the Requirement given the specific facts and circumstance of its use, ownership or operation of the Bulk- Power System.” While we agree with Northern Indiana that, depending on the Requirement in question, in some instances (such as active system testing) **documentation would suffice to demonstrate compliance, even in these cases auditors should look at the content of the documentation to determine if the substance of the Requirement has been met.**

73. Xcel seeks clarification regarding responsible entities that comply with the substance of a Requirement but violate the documentation provisions. In Order No. 693, in response to a similar request by Xcel, the Commission explained that, “[w]hile the Commission generally agrees that it is a violation of the Requirements that is subject to a penalty, we recognize that because Measures are intended to gauge or document compliance, failure to meet a Measure is almost always going to result in a violation of a Requirement.” **We add that a responsible entity's failure to maintain documentation (as set forth in a Measure) that obstructs the ability of the ERO, Regional Entity or Commission to determine compliance with the substance of a Requirement may warrant a penalty.**

74. In the CIP NOPR, the Commission also noted that, while certain Requirements of the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, the Requirements do not always explicitly require implementation of the plan, policy or procedure. The Commission proposed to interpret such provisions to include an implicit implementation requirement.

75. Consistent with that proposal, the Commission concludes that, **where the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, there should be a corresponding obligation to implement the plan, policy or procedure.** However, while the CIP NOPR proposed to interpret the CIP Reliability Standards as including an implicit obligation to implement plans, policies and procedures, we are persuaded by the commenters that a better approach is for the ERO to

develop modifications to the CIP Reliability Standards that contain appropriate implementation language. Accordingly, we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards.

76. As to Xcel's argument that, at times, the proper course is to deviate from a plan, we agree that the details of such plans are not equivalent to Requirements of a CIP Reliability Standard. However, the responsible entity's plan should be followed unless a deliberate decision is made for good reason not to follow it. Such reason should be documented and available for compliance auditors to review. Merely ignoring plan provisions is equivalent to not having a plan. For clarity, we note that a decision not to follow a particular plan provision due to circumstances will not except a responsible entity from a related Requirement in a CIP Reliability Standard. As discussed below, we find that any exception to a CIP Reliability Standard must comply with the required conditions for a technical feasibility exception.

77. In the CIP NOPR, the Commission explained that, because the CIP Reliability Standards are new and require applicable entities in many cases to develop new cyber security systems and procedures, NERC developed an implementation plan based on a schedule that provides for implementation of the CIP Reliability Standards over a three year period. The implementation plan sets out a proposed schedule for accomplishing the various tasks associated with compliance with the CIP Reliability Standards. The schedule gives a timeline by calendar quarters for completing various tasks and prescribes milestones for when a responsible entity must: (1) "begin work;" (2) "be substantially compliant" with a Requirement; (3) "be compliant" with a Requirement; and (4) "be auditably compliant" with a Requirement. According to the implementation plan, "auditably compliant" must be achieved in 2009 for certain Requirements by certain responsible entities, and in 2010 for others

86. The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities to achieve auditable compliance. Responsible entities require a reasonable period of time to purchase and install new cyber software and equipment and develop new programs and procedures to achieve compliance. Commenters indicate that the implementation plan provides that reasonable period of time. Further, we agree with commenters that there is an urgent need to move forward without any delays. Accordingly, we approve NERC's implementation plan.

87. Commenters raise concerns regarding the impact on the implementation plan of the Commission's directives for modifications to the CIP Reliability Standards. As explained above, the Commission is not modifying the CIP Reliability Standards in this Final Rule. Rather, pursuant to section 215(d)(5) of the FPA, the Commission in the Final Rule directs the ERO to develop certain modifications to the CIP Reliability Standards pursuant to the NERC Reliability Standards development process. Even though the development of such modifications will take time, this does not present a reason for delay or revision to the NERC implementation plan for implementing the CIP Reliability Standards approved in this Final Rule.

88. The Commission believes that the modifications to the CIP Reliability Standards developed by the NERC Reliability Standards development process should not be audited prior to the conclusion of the approved implementation plan. EEI and other commenters claim that commencing the development of such modifications prior to the conclusion of the implementation plan would be discouraging to industry. The Commission, however, finds that it is unacceptable to delay the development of the modifications directed in this Final Rule until after the conclusion of the implementation plan. Since it is uncertain how long it will take to develop revised CIP Reliability Standards, we believe it is not reasonable to wait until the 2009-2010 time period for the process to start. Features such as enhanced conditions on technical

feasibility exceptions and oversight of critical asset determinations are too important to the protection of the Bulk-Power System to wait that long.

89. While we are both sympathetic and concerned about straining industry resources, the Commission and the electric industry must do their best to protect the electric infrastructure that is essential to the health and safety of the nation. Therefore, we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule. As suggested by NERC, the Commission will consider a second implementation plan for achieving compliance with the forthcoming revised CIP Reliability Standards.

90. The Commission did not propose to remand CIP-002-1 as argued by Entergy. Nonetheless, Entergy raises a valid concern since the Commission's directive, discussed below, that the ERO develop modifications to CIP-002-1 could affect a responsible entity's identification of critical assets. We share Entergy's concern that there are threshold issues regarding CIP-002-1 that must be addressed before responsible entities can have certainty regarding which assets must be protected according to the CIP Reliability Standards. We also believe that responsible entities need certainty regarding the conditions for a technical feasibility exception to inform their decisions about how to comply with the CIP Reliability Standards, even in their current form. Therefore, we direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.

96. While the Commission is sensitive to concerns that more frequent self certifications may be burdensome, it is important that the ERO and the Commission know whether industry, or segments of industry, are having difficulty implementing the CIP Reliability Standards. Therefore, we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required. Such additional self-certifications may be a "stream-lined" version, but must be useful for the ERO and the Commission to assess industry's progress toward achieving compliance with the CIP Reliability Standards.

97. Further, we adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify. The ERO and the Regional Entities should then work with such an entity either informally or, if appropriate, by requiring a remedial plan to assist such an entity in achieving full compliance in a timely manner. Further, we expect the ERO and the Regional Entities to provide informational guidance, upon request, to assist a responsible entity in assessing its progress in reaching "auditably compliant" status.

98. With regard to METC-ITC's comment, we will not require NERC and the Regional Entities to submit plans describing how it will undertake these responsibilities. Rather, the ERO and Regional Entities can address any need for additional resources in the ERO's annual budget filing. If necessary to fulfill their statutory obligations, the ERO and Regional Entities may file a request for additional funding to supplement their Commission approved budgets.

99. With regard to SDG&E's comment, we clarify that the goal of a Regional Entity working with a responsible entity that is unable to self-certify is to assist the entity in meeting the NERC time frames for auditable compliance, and not to accelerate compliance ahead of schedule.

101. "NERC and other commenters oppose the addition of a cyber security assessment to NERC's existing readiness review..."

105. The Commission is persuaded by comments regarding the limited reach of readiness reviews and the questionable utility of such reviews prior to the date by which entities are to be compliant; thus, adding the CIP Reliability Standards to the readiness reviews at this time will delay industry's compliance efforts. Therefore, the Commission will not require that the CIP Reliability Standards be added to the readiness reviews at this time.

111. "...cost can be a valid consideration in implementing the CIP Reliability Standards."

128. Consistent with the CIP NOPR, the Commission concludes that the concept of reasonable business judgment is inappropriate in the context of mandatory CIP Reliability Standards. Accordingly, the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.

129. While there may have been no intention to import corporate law concepts into the CIP Reliability Standards, it is difficult to draw any other conclusion on the basis of the documents provided. We note that the only guidance on reasonable business judgment that emerged from the Reliability Standards development process and that was supplied to the Commission is found in the FAQ document, and that document appears to invoke the traditional corporate law business judgment rule. The FAQ document specifically references existing court precedent on the rule, and it sets forth the elements of reasonable business judgment in what is essentially a restatement of classic formulations of the business judgment rule. Moreover, the FAQ document specifically references one of the most objectionable aspects of the business judgment rule in the cyber security context, the requirement that the courts defer to the decisions of company officers and directors in all but the most extreme circumstances.

130. In short, the only explanation of reasonable business judgment in the documentation responsible entities would rely on focuses on corporate law concepts. We thus reject Mr. Brown's claim what we are being hyper-legalistic and constructing straw men rather than addressing the clear intent of the language. Mr. Brown fails to identify where some intent other than to adopt the traditional business judgment rule is clearly stated, and his references to 200 years of legal precedent only serve to reinforce our conclusion. We are unaware of any such extensive body of precedent on reasonable business judgment other than that developed in the corporate law context.

131. The most common argument raised in favor of reasonable business judgment is that it ensures flexibility. The Commission, however, acknowledged the importance of flexibility and discretion in the CIP NOPR. The CIP Reliability Standards consist for the most part of quite general Requirements that must be implemented in a wide variety of circumstances. As drafted, they do not provide one-size-fits-all solutions and, rather, require responsible entities to assess their individual situations and devise solutions appropriate to their circumstances. We therefore disagree with Ontario Power that outright removal of all references to reasonable business judgment would render the CIP Reliability Standards too rigid. It will still be necessary for responsible entities to choose between available alternatives to arrive at cyber security solutions that best fit their situation. In short, the CIP Reliability Standards do not simply allow flexibility, they require it.

132. Many commenters suggest that the issue is not simply flexibility, but rather the flexibility to balance costs against other factors when implementing the CIP Reliability Standards. Many of the arguments about cost have been raised in connection with the problem of technical feasibility as it relates to long-life legacy equipment. We will address that issue below and note here simply that cost is a relevant

consideration for those purposes, and recourse to reasonable business judgment is unnecessary to confirm that or to address the problem appropriately. Beyond that we disagree that deleting references to reasonable business judgment will lead to overly burdensome requirements or counterproductive results. For example, we disagree with Tampa Electric that without the leeway afforded by reasonable business judgment responsible entities would be forced into cost-prohibitive controls that do not add value in terms of security. No explanation was provided as to how this might occur. The Commission acknowledged the validity of cost considerations in the CIP NOPR and reaffirms that position here. The funds available for cyber security will not be infinite and, therefore, a responsible entity will need to make careful judgments to ensure that available funds are spent effectively. We do not see how the absence of references to reasonable business judgment will prevent this from happening.

133. Finally, some commenters link the need for flexibility with the problem of liability. We are keenly aware that unlike many other aspects of Bulk-Power System operations, cyber security represents a new and rapidly developing field. In other areas, the substance of appropriate practices is well established and well understood, but there can be considerably more uncertainty in the cyber security realm. Responsible entities therefore quite understandably wish to have, in Entergy's words, assurances that their actions meet the CIP Reliability Standards and Requirements if they act in good faith, perform the proper evaluation, and act consistent with their evaluation. We agree that they should have such assurances, but we disagree that references to reasonable business judgment are an appropriate way to provide such assurances. The real issue is whether responsible entities take reasonable and prudent actions based on an informed understanding of the current state of cyber security practice and how it applies to their situation. The Commission, therefore, disagrees with AMP-Ohio and Mr. Brown that the absence of references to reasonable business judgment will lead to a strict liability enforcement regime.

134. We disagree with Mr. Brown's claim that removal of reasonable business judgment could lead to liability for individual managers under section 215 of the FPA. That section applies to users, owners, and operators of the Bulk-Power System, and any liability arising under section 215 applies to them, not their employees.

135. Although we disagree with National Grid and others that alternative language is necessary to ensure necessary flexibility, we agree that the ERO and the participants in the Reliability Standards development process may choose to develop alternative language to replace reasonable business judgment and propose it for Commission approval. Such language would need to be adapted to the issues involved in forming judgments on proper cyber security measures and embody an objective standard focused on conduct that promotes the interests of Bulk-Power System security and reliability. Such language would also need to take into consideration our finding discussed below that a responsible entity cannot excuse itself from compliance with a requirement of the CIP Reliability Standards.

136. In response to the Southwest TDUs, we note that the CIP Reliability Standards apply in the same way to both public and private users, owners, and operators of the Bulk-Power System. Any specific issues that Southwest TDUs have with the Reliability Standards should be raised in the Reliability Standards development process.

137. Finally, we reject arguments that we are being overly prescriptive in directing the ERO to remove all references to reasonable business judgment from the CIP Reliability Standards. We discuss that general issue elsewhere in this Final Rule and will not repeat that discussion here. It is, however, important to note that such objections are inapposite in this instance for an additional reason that involves the specific nature of the issue raised. The concept of reasonable business judgment speaks to a general legal standard of conduct proposed to apply under a statute that Congress has directed the Commission to administer. It does not involve matters specific to reliability but rather is bound up with the problem of legal

enforceability. The Commission has a particular duty to see that the laws it administers can be enforced effectively. We are not being overly prescriptive when acting to ensure that this will be the case.

138. Based on the above discussion, as well as our lengthy analysis in the CIP NOPR, the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.

150. The Commission continues to view the term “acceptance of risk” as representing an uncontrolled exception from compliance that creates unnecessary uncertainty about the existence of potential vulnerabilities. Responsible entities should not be able to opt out of compliance with mandatory Reliability Standards. The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.

151. In response to concerns raised by NERC, EEI and others, we agree that this action should occur through the Reliability Standards development process. In response to the concerns of many commenters who argue that it should be possible to propose alternative language, we note that this is consistent with the Reliability Standards development process. However, any alternative language that provides a similar opportunity for a responsible entity to opt out of compliance would be subject to remand. Rather, the Commission believes that alternative language that deals with such issues in terms of technical feasibility is preferable. To that end, we have adapted the concept of technical exceptions to encompass a broader range of valid justifications. Elsewhere in this Final Rule we address the criticism that our actions are overly prescriptive and those remarks apply equally here.

152. Expanding the use of the technical feasibility conditions would address the desire for flexibility expressed by some commenters while providing the control that the Commission finds to be necessary. It would provide for documentation, reporting and approval of how responsible entities have elected to comply with the CIP Reliability Standards and thus would permit the ERO and Regional Entities to assess the significance of any possible vulnerability. As to the argument by METC-ITC that a technical feasibility exception may not be possible in all cases, we note that we have found that technical feasibility should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable. Thus, this approach addresses the issue of inadequately tested patches raised by APPA/LPPC, and similar general concerns raised by Tampa Electric.

153. In response to Entergy, we note that a long-established practice of risk acceptance by senior management does not mean that a continuation of this practice is appropriate under a new system of mandatory cyber security Reliability Standards. We have addressed Entergy’s concerns about costs-related legacy equipment in connection with technical feasibility.

154. Many commenters defend retention of the acceptance of risk language by pointing out that it is impossible to eliminate all risk. While likely true, it is beside the point. The acceptance of risk language in the CIP Reliability Standards fails to acknowledge that the real issue is whether the nature and level of inevitable risk is acceptable from a systemwide perspective. Within a system of CIP Reliability Standards intended to protect the Bulk-Power System as a whole, that problem can be addressed by a system that documents and reports the risks in question and ultimately subjects them to approval by the ERO or Regional Entities. The Commission’s concern in the CIP NOPR was with the lack of appropriate controls, and eliminating references to acceptance of risk does not imply that all risk can be eliminated.

155. We disagree with Mr. Brown that mutual distrust means that risks accepted by one entity do not affect others on an interconnected control system. A mutual distrust approach is a good security posture. However, its value depends on how well it is implemented. There will likely be a variety of levels of

sophistication applied to implementing mutual distrust. It is not a basis for allowing other responsible entities to ignore their obligations under mandatory CIP Reliability Standards.

156. Accordingly, the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.

178. The Commission adopts the CIP NOPR proposal and directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. We will modify some of our proposed criteria for that framework of accountability further below. We are persuaded by commenters that the proposed conditions for invoking the technical feasibility exception should allow for operational considerations. In response to Northern Indiana and other commenters, we note that the Commission did not propose to eliminate references to technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly and without reference to considerations of business judgment.

179. In response to those commenters who argue that the Commission's concerns and directives should be addressed through the Reliability Standards development process, we agree that to the degree revisions to the Reliability Standards are necessary to address our concerns, they would be made through that process. We disagree, however, with the arguments that claim we are rewriting the CIP Reliability Standards or adhering to a one-size-fits-all approach. With respect to the latter point, we note that technical feasibility issues are by their nature something that must be dealt with on a case-by-case basis, as they only arise in specific circumstances. Our concern here is primarily with the framework within which decisions on technical feasibility are made and ensuring that this framework promotes sound decisions that lead to effective results. The oversight provisions we describe below are essential elements of such a framework.

180. We agree with NERC and other commenters on the underlying rationale for a technical feasibility exception, i.e., that there is long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are an acknowledged concern. While equipment replacement will often be appropriate to comply with the CIP Reliability Standards, such as in instances where equipment is near the end of its useful life or when alternative or supplemental security measures are not possible, we acknowledge that the possibility of being required to replace equipment before the end of its useful life is a valid concern.

181. The Commission, however, disagrees with Northern Indiana that technical feasibility should be interpreted to apply to future assets also. The justification presented for technical feasibility exceptions is rooted in the problem of long-life legacy equipment and the economic considerations involved in the replacement of such equipment before the end of its useful life. We recognize that these considerations can be valid in some cases, but Northern Indiana has not explained why technical feasibility exceptions should apply to replacement equipment. The Commission neither assumes that technical infeasibility issues will be present only during the transition period, nor does it assume that on a going forward basis there will be only one single means to comply with the CIP Reliability Standards. It does assume, however, that all responsible entities eventually will be able to achieve full compliance with the CIP Reliability Standards when the legacy equipment that creates the need for the exception is supplemented, upgraded or replaced.

182. The Commission agrees with various commenters that the implementation of the CIP Reliability Standards should not be permitted to have an adverse effect on reliability and that proper implementation requires that care be taken to avoid unintended consequences. We thus believe it is important to clarify

that the meaning of “technical feasibility” should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable.

183. We disagree with Mr. Brown’s view that whether or when to replace equipment that cannot do something due to technical feasibility with equipment that can do so is purely a managerial decision, especially since he intertwines this proposition with the concept of reasonable business judgment. While we accept NERC’s rationale for technical feasibility exceptions, as discussed below, an integral issue in individual cases where legacy equipment presents a technical feasibility issue is whether an alternative course of action protects the reliability of the Bulk-Power System to an equal or greater degree than compliance would. This is not a purely managerial decision involving reasonable business judgment, regardless of what meaning one imparts to that term.

184. While a number of commenters agree that it is important to clarify the meaning of technical feasibility, none appear to support defining the term in the NERC Glossary. Therefore, in light of the comments received generally and the specific guidance that we are providing to the ERO in connection with technical feasibility, we conclude that a definition of this type is unnecessary. A definition cannot substitute for a framework of conditions or criteria to provide accountability, and if those conditions or criteria are implemented, a definition is not needed. We do not agree with NERC that replacing the term technical feasibility with “exemption for reliability” would be helpful. We note, in particular, that an “exemption” normally is understood to be a release from an obligation whereas what is under discussion here is an exception that forms an alternative obligation.

185. While the Commission will not address the merits of any particular technology, we note that Teltone’s comments raise an important general consideration when developing policy on technical feasibility. While technical limitations present real issues, and while one should not be overly optimistic that technological developments will resolve them sooner than expected, one should not be overly pessimistic either. Indeed, high standards should, if anything, encourage the development of technical solutions.

186. Based on the above considerations, the Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place. The term technical feasibility should be interpreted narrowly to not include considerations of business judgment, but we agree with commenters that it should include operational and safety considerations

192. With some minor refinements discussed below, the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception. While the CIP NOPR proposed that each remediation plan contain a reasonable completion date, the Commission is persuaded by the comments of National Grid and SPP that a date certain for remediation may not be possible in some instances. While we expect remediation by a date certain to be the norm, we will not require a date certain for remediation in every instance that a responsible entity invokes the technical feasibility exception. An entity must provide an explanation when it believes that it is not possible for a remediation plan to provide a reasonable completion date.

193. We also agree with Northern Indiana that in some instances remediation can be required only to the extent possible. For example, in some cases it may never be possible to enclose certain critical cyber assets within a six-sided physical boundary as required under CIP-006-1. However, such cases need to be sufficiently justified, the mitigation strategies must be ongoing and effective, and the justification must be subject to periodic review. We also are mindful that accelerated replacement of equipment can be economically wasteful where security is not otherwise compromised. We thus agree with National Grid that where mitigation measures are as or more effective than compliance, and in the case of minor technical or administrative requirements, replacement of certain assets before the end of their useful lives can be wasteful and inefficient. We also agree with SPP that remediation might not be necessary where compensating measures are equally effective in reducing risk. However, such cases must be subject to clear criteria and periodic review and, where necessary, updates.

194. However, in adopting this approach, we do not intend to suggest that it would never be necessary to replace equipment before the end of its useful life to achieve cyber security goals. Where equipment is near the end of its useful life or if insufficient mitigation measures are available, the equipment should be replaced. However, such situations must be dealt with on a case-by-case basis. We emphasize that responsible entities must protect assets that are critical to the reliable operation of the Bulk-Power System.

209. For the reasons discussed below, the Commission concludes that technical feasibility exceptions should be reported and justified and subject to approval by the ERO or the relevant Regional Entity. The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria. However, because we are persuaded by the commenters, we have modified certain elements of our original proposal, as discussed below.

210. Most objections to the CIP NOPR proposal regarding the review and approval of technical feasibility exceptions are not objections in principle but rather focus on practical issues of implementation, such as limited ERO and Regional Entity resources and sensitivity of the information in question. To the extent that objections in principle have been raised, we disagree. Thus, we disagree with ReliabilityFirst's argument that senior manager approval of exceptions is unnecessary because of the responsibilities already assigned to the senior manager by CIP-003-1. These technical feasibility exceptions implicate matters that go beyond the purview of individual responsible entities and must be subject to review and approval by those with a wider-area view and general responsibility for system reliability. We also disagree with the ISO/RTO Council that the Commission should simply direct the ERO to detail the type of justifications and considerations that must be documented when invoking a technical feasibility exemption. While such guidance could be useful, it cannot substitute for reporting, review, and approval, which is necessary to address concerns that extend beyond the reach of an individual responsible entity.

211. With regard to the senior management approval, we continue to believe that internal approval is an important component of an overall framework of accountability with regard to use of the technical feasibility exception. Therefore, we adopt this aspect of our CIP NIPR proposal and direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.

212. However, the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed. We agree, in particular, with those commenters who argue that pre-approval could tax ERO and Regional Entity resources, delay implementation, and possibly create undue risks that sensitive information will be disclosed.

213. The Commission agrees with National Grid that **Regional Entities should, in the first instance, receive and catalogue notices of technical feasibility exceptions that are claimed.** Such notices must include estimates of the degree to which mitigation measures achieve the goals set by a CIP Reliability Standard and be in sufficient detail to allow verification of whether reliance on exceptions (or the associated mitigation measures) **adequately maintains reliability and does not create reliability issues for neighboring systems. Initial submission of notices should be provided by responsible entities at least by the “Compliant” stage of implementation in order to allow Regional Entities to plan for auditing exceptions,** as described in more detail below.

214. The Commission also agrees with National Grid, EEI and others **that actual evaluation and approval of technical feasibility exceptions should be performed in the first instance in the audit process.** This would allow assessment of exceptions within their specific context and thus facilitate greater understanding in evaluating individual exceptions, as well as related mitigation steps and remediation plans. This also would increase the amount of sensitive information that remains on-site and reduces the risk of improper disclosure. In addition, it will **allow the ERO and Regional Entities, informed by the initial notices discussed above, to include personnel in audit teams with sufficient expertise to judge the need for a technical feasibility exception and the sufficiency of preferred mitigation measures.**

215. Given the significance of technical feasibility exceptions, the Commission believes that **initial audits of technical feasibility exceptions should be expedited, i.e., performed earlier than otherwise, including moving the audit to an earlier year.** Also, in general, responsible entities claiming such exceptions should receive higher priority when determining which entities to audit, and the more exceptions an entity has, the higher the priority for audit should be. Further, **NERC may provide an appeals process for the review of technical feasibility exceptions, if it determines that this is appropriate.**

216. However, the Commission notes that the audit process is a Regional Entity and ERO process, and audit team findings regarding exceptions are subject to Regional Entity and ERO review. The Commission believes that the **audit report should form the basis for ERO or Regional Entity approval of individual exceptions.** Approval thus represents a determination on compliance with the applicable CIP Reliability Standards, and we disagree with the ISO/RTO Council that approval of technical feasibility exceptions raises any conflict of interest or due process concerns. The proposed procedures raise no special issues in this respect.

217. We agree with EEI and others that approvals and potential appeals should not be allowed to delay implementation, but we believe our revised proposal resolves this problem. We also agree with APPA/LPPC that responsible entities should be able to rely on a technical feasibility exception prior to formal approval. However, we disagree with Northern Indiana that penalties should be waived within the time when an approved remediation plan is being implemented, as proper implementation of the plan itself constitutes a necessary element of compliance.

218. In summary, on the issues **pertaining to external approval of a responsible entity’s use of the technical feasibility exception, rather than a pre-approval process, we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.** This process should **require the ERO or a Regional Entity to approve any technical feasibility exception, taking into account whether the technical feasibility exception is needed and whether the mitigation and remediation steps are adequate to the circumstance.**

219. We agree with comments emphasizing the importance of protecting sensitive information relating to technical feasibility exceptions. We agree with SPP and others that CEII treatment should be available for

any such information. In response to Bonneville, we agree that a governmental entity subject to FOIA requirements should not be required to submit sensitive information about critical assets or critical cyber assets that could be deemed a waiver of FOIA protection that is otherwise available. Nonetheless, a governmental entity's decision to rely on a technical feasibility exception should also be subject to appropriate oversight and accountability. Thus, we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.

220. As stated in the CIP NOPR, the Commission believes that it is important that the ERO, Regional Entities and the Commission understand the circumstances and manner in which responsible entities invoke the technical feasibility exception. Accordingly, we direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability. The annual report must address, at a minimum, the frequency of the use of such provisions, the circumstances or justifications that prompt their use, the interim mitigation measures used to address vulnerabilities, and efforts to eliminate future reliance on the exception.

221. While we agree with commenters that the compilation of data for the annual report must not compromise the security of the Bulk-Power System, we disagree that this is a reason not to require the report. Rather, as we indicated in the CIP NOPR, the report should not provide a level of detail that divulges CEII data. Rather, the report should contain aggregated data with sufficient detail for the Commission to understand the frequency with which specific provisions are being invoked as well as high level data regarding mitigation and remediation plans over time and by region. Further, we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.

222. In conclusion, pursuant to section 215(d)(5) of the FPA, we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards. As discussed above, structural elements of this framework include mitigation steps, a remediation plan, a timeline for eliminating use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects the technical feasibility exception on the reliability of the Bulk-Power System. We direct the ERO to develop appropriate modifications, as discussed above.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability

Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

236. ... the commission approves Standard CIP-002-1 as mandatory and enforceable.

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

254. Commenters raise a number of topics that they believe should be addressed in the NERC guidance, such as how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary. We believe these are all appropriate topics to be addressed and direct the ERO to consider these commenter concerns when developing the guidance.

255. The Commission proposed in the CIP NOPR that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. While we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.

256. Regarding MidAmerican's comments on use of the N minus 1 criterion when applying a risk-based assessment methodology to the identification of critical assets, we agree with MidAmerican that an N minus 1 criterion is not an appropriate risk-based assessment methodology for identifying critical assets. While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk based assessment in CIP-002-1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. Also, we note that the definition of "critical assets" is focused on the criticality of the asset, not the likelihood of an outage. Based on this reasoning, in response to US Power, we clarify that a generator

should not assume that none of its individual generating assets would be regarded “critical” to the Bulk-Power System.

Footnote 84: Further, Requirement R.1.2.3 provides that the risk-based assessment must consider “generation resources that support the reliable operation” of the Bulk-Power System. This language indicates that certain generation facilities, and presumably some facilities within a region identified as critical, must be considered in an assessment. Beyond this, we leave it to the ERO to provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset. As discussed later in the Final Rule, the Commission will monitor and evaluate the outcome of this endeavor – the list of critical assets.

257. With regard to Xcel’s request for clarification regarding the meaning of the phrase “used for initial system restoration,” in CIP-002-1, Requirement R1.2.4, we direct the ERO to consider this clarification in its Reliability Standards development process.

258. As to Entergy’s suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California’s suggestion that the ERO establish a formal “feedback loop” to assist the industry in developing policies and procedures.

270. As discussed above, commenters that address the subject uniformly oppose the CIP NOPR statement that “marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process the data, would be considered critical cyber assets” subject to the CIP Reliability Standards. These commenters contend that marketing data typically does not qualify as a critical cyber asset and the Commission’s proposal is beyond the current scope of the CIP Reliability Standards. Moreover, several commenters suggest that some data and support systems may fit the definition of critical asset and, thus, supporting critical cyber assets must comply with CIP-002-1.

271. The Commission remains concerned that, while not all marketing data or other data may be considered a critical cyber asset essential to the proper operation of a critical asset, there may be times where it is properly classified as such. For example, if a critical asset is configured such that it cannot operate and support the reliability and operability of the Bulk-Power System without a real-time stream of data, that data fits the definition of a critical cyber asset, and should be protected. Once a particular piece of data is no longer needed by the critical asset, it is no longer a critical cyber asset. On this point, we agree with commenters that there is a temporal characteristic to data as a critical asset.

272. Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper’s comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.

273. The Commission also agrees with ISO-NE that experience in the implementation of the CIP Reliability Standards may indicate a need to further address this topic in a future proceeding.

279. The Commission accepts the explanation of the ERO and ReliabilityFirst that a control system could be a critical cyber asset, but not a critical asset.

280. The Commission has two concerns regarding the misuse of facilities, and clarifies those concerns here. First, Requirement R1.2.1 requires responsible entities to consider control centers and backup control centers as potential critical assets. In determining whether those control centers should be critical assets, we believe that responsible entities should examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks. Responsible entities should also examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on the reliability of the Bulk-Power System. The Commission recognizes that, when these matters are taken into account, it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset.

281. Second, the Commission is concerned about the misuse of a control system that controls more than one asset. The assets could be multiple generating units, multiple transmission breakers, or perhaps even multiple substations. All of the controlled assets could be taken out of service simultaneously due to a failure or misuse of the control system. Individually, perhaps none of the controlled assets would be considered as a critical asset. However, with a simultaneous outage due to the single point of control, the controlled assets might affect the reliability or operability of the Bulk-Power System and, therefore, should be considered as critical assets. In that case, the common control system should be considered a critical cyber asset.

282. Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets. The clarification of our concern over misuse of control systems addresses Entergy's comment on this issue as well.

283. The Commission concurs with SPP that both insider and external threats should be considered as part of a risk-based assessment.

284. We share Applied Control Solutions' concern that too few assets may be identified as critical cyber assets. However, there is no evidence that will be the case, and there is no formally accepted method for identifying critical cyber assets before us at this time. Therefore, we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time. The Commission may revisit this circumstance in a future proceeding.

285. As to the conflicting comments of ISA99 Team and Energy Producers, Requirement R2 of CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial-up access. Energy Producers argues that Requirement R2 should be retained, while ISA99 Team argues that devices that use non-routable protocols should also be considered as possible critical cyber assets. We do not find sufficient justification to remove this provision at this time. However, we direct the ERO to consider the comment from ISA99 Team. We also do not find sufficient justification to order the inclusion of communication links in CIP-002-1 at this time.

288. To clarify, the Commission did not propose to direct that the ERO develop a requirement for responsible entities to document why each specific asset was identified or not identified as "critical." Rather, the Commission's intent was that a responsible entity must be able to explain such

determinations, for example upon inquiry by an auditor, to confirm compliance with the Reliability Standard. Nonetheless, we are persuaded by the commenters that the documentation of a responsible entity's risk-based assessment methodology pursuant to Requirement R1.1 and the results of its annual application of the methodology pursuant to Requirement R2 should suffice to explain a responsible entity's asset determinations. Accordingly, the Commission will not direct the ERO to develop a modification to address this concern. However, if experience shows that responsible entities are failing to consider in their assessments specific types of assets that the Commission, ERO or others believe should be included in an assessment and therefore not in compliance with the Reliability Standard, there may be a need to revisit this matter in the future.

294. The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology. This determination is consistent with the Blackout Report's recommendation to establish clear authority and ownership for physical and cyber security. Further, regardless of whether the current Requirements implicitly require senior manager review of the assessment methodology, we believe the matter is too important to rely on inference. Accordingly, the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.

295. With regard to Northern Indiana's concerns, we are not directing a revision to the current language of Requirement R4 which provides for "the senior manager or delegate(s)'s approval" of the list of critical assets and list of critical cyber assets. As we understand the provision, the senior manager still retains ultimate responsibility for the determinations of his or her delegate(s). Otherwise, senior management could avoid responsibility by 'delegating downward.'

296. With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."

297. In response to comments by Bonneville and NRECA, the Commission clarifies that we do not intend that an individual employee of a user, owner or operator of the Bulk-Power System will be subject to a penalty pursuant to section 215 of the FPA because a responsible entity violates a CIP Reliability Standard. This matter is addressed in more detail in our discussion of CIP-003-1.

319. The Commission affirms its CIP NOPR determination that responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large - in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility.

320. We will not allow a "safe harbor" for good faith compliance as requested by AMP Ohio. We do not believe that blanket waivers from an enforcement action are appropriate in this context and have

previously denied other requests for safe harbors from enforcement. Rather, we believe that **demonstrable good faith compliance is a legitimate mitigating factor in an enforcement action.**

321. SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system.

322. The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists. The Commission finds that an external review of critical assets by an appropriate organization is needed to assure that such lists are considered from a wide-area view (i.e., from a regional perspective) and to identify trends in critical asset identification. Further, while we recognize that individual circumstances may likely vary, an external review will provide an appropriate level of consistency.

323. The Commission disagrees with the suggestion of Luminant and others that external review should be voluntary. The identification of critical assets pursuant to CIP-002-1 is crucial to cyber security protection because this determination controls whether a responsible entity must comply with the remaining CIP requirements in CIP-003-1 through CIP-009-1. External review will help ensure that responsible entities have an accurate and complete list of critical assets, which will in turn allow them to be appropriately protected to further the security of the nation's Bulk-Power System. Allowing external review as a voluntary measure is not adequate to ensure that responsible entities are prepared to address cyber vulnerabilities and cyber threats. Based on the same reasoning, we reject the suggestion of Northern Indiana and others that the external review should only address the assessment methodology, and not critical asset lists.

324. The Commission also disagrees with commenters who insist that the external review can be performed pursuant to the ERO's and Regional Entity's current compliance and enforcement programs, and the audit process in particular. While the Commission decided earlier in the Final Rule to rely on the ERO and regional audit processes to examine exceptions to compliance based on "technical feasibility," the Commission does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations. Review of critical asset lists through individual audits would span a significant period of time, measured in years, during which time such lists would not undergo review and possibly gaps in security could result. While EEI's suggestion of spot checks prior to the "auditably compliant" stage would provide more timely feedback it would, by design, not be comprehensive. The Commission concludes that a structured program for the formal, timely review of critical assets lists is a reasonable means to provide timely, comprehensive guidance to responsible entities on the adequacy of their critical asset lists.

325. The Commission agrees with Ontario IESO that in a dispute between a responsible entity and the external reviewer over whether to identify an additional asset as critical, the external reviewer should prevail. (However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets.) We recognize, however, that there may be a legitimate reason for a responsible entity to dispute such a determination, possibly through an appeal. We leave it to the ERO to determine the need for such an appeal mechanism and, if appropriate, the development of appropriate procedures (or reliance on appeal procedures currently provided in the NERC Rules of Procedure). While the ERO may determine

that an appeals process is a necessary aspect of this program, we do not believe that the burden of such appeals outweighs the benefits of the external review of critical asset lists.

326. The Commission in the CIP NOPR proposed that the Regional Entities be responsible for the external review of critical asset lists, and also expressed a willingness to consider a review process that allows for the participation of other organizations such as reliability coordinators and transmission planners. As indicated above, a number of commenters question whether the Regional Entities have the expertise or resources to conduct the reviews. Rather, there was considerable support for reliability coordinators conducting the external review because of their technical expertise, their wide-area view and their role of coordinating among neighboring systems.

327. The Commission believes that the Regional Entities must have a role in the external review to assure that there is sufficient accountability in the process. Further, a Regional Entity role is necessary because the Regional Entities and ERO are ultimately responsible for ensuring compliance with Reliability Standards. For example, if the ERO determines that an appeals process is needed, this process cannot rest with an active owner or operator of the Bulk-Power System such as a reliability coordinator. Moreover, the ERO and the Commission have oversight authority of the Regional Entities' programs and procedures pursuant to section 215 of the FPA.

328. Beyond the direction that the Regional Entities maintain a role in the external review to process to assure that there is sufficient accountability, we leave to the ERO to determine whether the Regional Entities have, or can timely develop, the resources to conduct the external reviews. Alternatively, the ERO may determine that another entity such as reliability coordinators may be best equipped to conduct the reviews. While commenters have made what the Commission believes to be a strong case that reliability coordinators are the appropriate entity to perform the reviews, the ERO should decide the best approach with its understanding of the capabilities and limitations of the Regional Entities. Regardless of this determination, however, the Commission notes that the Regional Entities have the oversight responsibility.

329. Based on the above discussion, the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.

330. The Commission agrees with commenters that critical asset lists contain sensitive information that needs to be protected from public dissemination. The Commission, however, does not believe that this concern is a persuasive rationale for not having an external review mechanism. Rather, adequate safeguards need to be developed to assure that the information contained in critical asset lists are not released during the external review process. While Requirement R4 of CIP-003-1 obligates a responsible entity to "implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets," the Commission does not view this as inherently conflicting with an external review process that has adequate safeguards to prevent the release of sensitive information.

331. In developing an appropriate external review mechanism, the ERO should include features for the controlled delivery of critical assets to the entity performing the external review. Likewise, the ERO should identify minimum safeguards that the external reviewer must deploy to protect sensitive information from disclosure. We agree with commenters' concern that the external reviewer should not become a "central repository" for critical asset lists, and this information should be returned to the responsible entity once the review is complete. The ERO should develop any other safeguards that it believes to be appropriate to protect the disclosure of sensitive information during the external review process.

332. CEA and Manitoba Hydro comment that some Canadian utilities are prohibited from sharing security information with U.S. authorities. They also note that some Canadian utilities regard sharing sensitive security information externally or with a foreign entity as a security risk. In response, the Commission's Final Rule only addresses the obligations of users, owners and operators of the Bulk-Power System in the United States (excluding Hawaii and Alaska). Accordingly, the Commission's directives regarding the development of an external review mechanism applies only to entities subject to the Commission's jurisdiction pursuant to section 215 of the FPA. Whether a similar review process is appropriate or lawful in other jurisdictions is beyond the scope of this Final Rule.

333. Bonneville comments that external review could result in FOIA concerns for Bonneville and other federal entities. It also cautions that external reviewers of critical federal security information may need federal security clearances before being allowed access to classified information. In response to Bonneville, we agree that a governmental entity subject to FOIA requirements should not be required to share sensitive information about critical assets lists that could be deemed a waiver of FOIA protection that is otherwise available. Nonetheless, a governmental entity's identification of critical assets should be subject to appropriate oversight. Thus, we direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information. The ERO should consult with governmental entities that are subject to the CIP Reliability Standards in developing such appropriate provisions and we, likewise, encourage Bonneville and other governmental entities to participate in the development of such provisions.

334. Further, if a governmental entity has classified material regarding its critical assets, this information may not be disclosed except in accordance with controlling laws and regulations. The ERO's external review process must explicitly recognize this limitation.

340. The Commission is sensitive to the concerns raised by the Congressional Representatives regarding the severe impact that a cyber attack on assets not critical to the Bulk-Power System could still have on the public. The Commission, however, believes that its authority under section 215 of the FPA does not extend to other infrastructure. Section 215 of the FPA authorizes the Commission to approve Reliability Standards that "provide for the reliable operation of the bulk-power system," which the statute defines as the facilities and control systems necessary for operation of an interconnected electric energy transmission network and the electric energy needed to maintain transmission system reliability. In addition, section 215(a)(1) specifically excludes from the definition of Bulk-Power System "facilities used in the local distribution of electric energy." Moreover, given the complexities surrounding this issue and the aggressive timeline that will be necessary merely to meet the more modest task of developing and implementing cyber security standards capable of protecting the reliability of the Bulk-Power System, we will follow the approach that we described in the CIP NOPR of approving CIP Reliability Standards designed to safeguard the reliability of the Bulk-Power System.

341. Although the Commission will not direct modifications to the scope of critical assets to be identified under CIP-002-1, for the reasons discussed above, the Commission agrees with commenters regarding the importance of considering interdependencies with other critical infrastructures. The Commission believes that to meaningfully address interdependencies with other critical infrastructures, it is important to coordinate with the stakeholders of these other infrastructures as well as with other government agencies and organizations. Thus, we affirm our CIP NOPR approach that "[w]hile broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help inform the electric sector and this Commission about the need for future Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation."

344. The commission approves reliability Standard CIP-003-1 as mandatory and enforceable...

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR – as well as the Final Rule – is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP-003-1 requires a responsible entity to document and implement a cyber security policy “that represents management’s commitment and ability to secure its Critical Cyber Assets.” The Requirement then states that the policy, “at a minimum,” must address the Requirements in CIP-002-1 through CIP-009-1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP Reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

357. Nor do we believe, as suggested by Idaho Power, that the proposed topics for guidance are better addressed by revisions to other Reliability Standards. Again, the guidance is in the context of securing critical cyber assets and is best addressed in the CIP Reliability Standards or a supporting guidance document.

358. In response to SoCal Edison, we disagree that guidance on topics such as power supplies, heating, and other equipment is too detailed for a corporate level policy. These topics are potentially relevant to securing critical cyber assets and, therefore, appropriate topics for guidance.

359. ISO/RTO Council, Ontario Power and other commenters raise concerns regarding potential civil penalty liability if a responsible entity addresses the additional guidance topics in its cyber security policy. The Commission does not believe that the inclusion of additional topics in the cyber security policy will increase a responsible entity’s penalty liability. We provide our views regarding the enforcement of cyber security policies below in addressing exceptions to such policies. In particular, we state there that our concern is that a good policy exists and that it is implemented through the exercise of sound reasoning. Consistent with the discussion in the following section, we do not believe that an entity’s decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result. We do require that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP-003-1.

360. We agree with APPA/LPPC that responsible entities cannot be expected to oversee the operations of commercial communications carriers. However, this is an example of precisely why more guidance would

be useful. Since responsible entities cannot oversee commercial communications carriers, it is important that they consider what they can do to guard against potential threats from that quarter.

372. The Commission continues to believe that it is important that there be ERO and Regional Entity oversight of exceptions from required security policies, however, the Commission agrees with commenters such as EEI and PG&E that this oversight is best accomplished through the existing Regional Entity oversight and audit process.

373. Requirement R1 of CIP-003-1 requires the development and implementation of a security policy. Requirement R3 provides that a responsible entity must document exceptions to its policy with documentation and senior management approval. The Commission is concerned that, if exceptions mount, there would come a point where the exceptions rather than the rule prevail. In such a situation, it is questionable whether the responsible entity is actually implementing a security policy. We therefore believe that the Regional Entities should perform an oversight role in providing accountability of a responsible entity that exempts itself from compliance with the provisions of its cyber security policy. Further, we believe that such oversight would impose a limited additional burden on a responsible entity because Requirement R3 currently requires documentation of exceptions.

374. That being said, the Commission agrees with EEI and others that Regional Entity review of exceptions to a responsible entity's cyber security policy is best accomplished pursuant to the existing Regional Entity audit process where all the relevant facts and circumstances can be considered. Further, review of exceptions to a cyber security policy in the audit process should effectively address commenter concerns regarding disclosure of sensitive information by keeping that data on site.

375. As we discuss elsewhere in the Final Rule, we agree with Bonneville regarding the need to preserve a governmental entity's FOIA protections and address security clearance concerns. The ERO should address these concerns through consultation with relevant governmental entities.

376. Further, the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not exempt responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves.

377. The Requirement to develop and implement a security policy differs from many other Requirements in that it is a means to the end of implementing those Requirements. Our concern that exceptions be documented and justified is primarily a concern that there be reasoned decision-making, consistency, and subsequent effectiveness in implementing the policy. We thus disagree with Northern Indiana that security policy exceptions which do not affect compliance with the Reliability Standards need not be documented. Further, in response to Entergy, as stated elsewhere in this Final Rule, our concern is that a good policy exists and that it is implemented through the exercise of sound reasoning. We do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result. We do require that the reasoning be documented to ensure that the responsible entity is indeed implementing the security policy as required by Requirement R1 of CIP-003-1.

378. In response to Northern Indiana's request for clarification of the information that would be required to justify an exception, we leave it to the ERO to provide guidance on the level of information that it considers appropriate, consistent with our discussion above.

381. The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA.

386. The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause.

387. In response to Northern Indiana, while we acknowledge that responsible entities are not authorized to enter private homes, we believe that an appropriate cyber security policy will ensure that such information is present in an employee's home only for legitimate reasons specified in the policy and should require the return of all information upon request.

397. Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP-003-1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

398. We agree with ISO/RTO Council that the phrase "verification that unintended changes have not been made" captures the core issue. Our concern is that some form of verification is performed to detect when unauthorized changes have been made and to identify those changes, as well as ensuring that the proper alerts are issued.

399. Many of the comments address practical issues involved in addressing accidental consequences and malicious actions, and we recognize that such issues exist. We, thus, agree with Puget Sound that change control and configuration management processes for critical cyber assets cannot ensure 100 percent integrity for those assets when making changes. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. However, we reject Puget Sound's proposal that the Reliability Standard should expressly recognize that absolute assurances are not required. We also believe that our revised directive to the ERO on Requirement R6 addresses Puget Sound's concern about the limitations imposed by a test environment.

400. In response to ReliabilityFirst and SPP, we understand that comprehensive regression testing is not necessary for every change regardless of how insignificant. We also agree with ISO/RTO Council that it

can be impractical and unnecessary to verify every intentional automatic change as it occurs. We believe that our revised directive to the ERO addresses these concerns.

407. The Commission proposed in the CIP NOPR that the ERO provide direction, i.e., guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world. The Commission noted that 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.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

409. We agree with Entergy that NIST provides much guidance, but we disagree that it is necessary to define the term mutual distrust. Our proposal is that there be guidance on certain issues and concerns, and we therefore do not believe that a formal definition advances that goal. In response to MidAmerican, we believe that clarification of the terms mutual distrust and outside world, as well as ensuring that any guidelines developed do not harm performance or reliability, are matters that the ERO should consider in the Reliability Standards development process.

410. We disagree with Northern Indiana that Reliability Standards CIP-005-1 and CIP- 007-1 address the matters of concern to us. Northern Indiana does not explain how these Reliability Standards provide guidance of the type we have described. We also disagree that the mutual distrust principle would require responsible entities to sever their communication links with their ISO or RTO or reliability coordinator. The principle could play a role in determining what precautions would need to be taken to protect those communications, but we do not see why it would lead to the specific result that Northern Indiana identifies. Mutual distrust does not imply refusal to communicate; it means the exercise of appropriate skepticism when communicating. The Commission believes additional guidance on what this means specifically in current practice would help responsible entities to avoid these misunderstandings.

411. We disagree with ISO-NE that guidance on mutual distrust is unnecessary because responsible entities either are compliant or they are not, mutual distrust notwithstanding. We do not see how responsible entities can fully understand the compliance issues they face without some understanding of how mutual distrust is applied in a modern security environment. Mutual distrust helps explain where an entity's responsibilities begin and end and what assumptions it can make about factors outside its control when it performs its risk-based assessment.

412. The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.

414. ...the Commission approves Standard CIP-004-1 as mandatory and enforceable.

431. The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.

432. The Commission notes that commenters did not provide specific reasons why employees should be granted access prior to training, but focused on the nature and scope of our proposed exceptions. Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power System. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.

433. Based on the concerns of commenters, the Commission modifies its CIP NOPR proposal that the ERO identify core training elements to ensure that essential training elements will not go unheeded in emergencies and in other compelling situations. While the Commission continues to believe that the identification of core training elements is useful, this issue would benefit from further vetting within the Reliability Standards development process. Thus, we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard. If the Reliability Standard development process determines not to identify core requirements, the ERO should provide an explanation of this decision. In reply to commenters, we clarify that by using the term core training our concern is for a responsible entity to pre-plan what information and training is necessary for personnel temporarily called in to help in an emergency – not that the actual scope of such training needs to be articulated in the Reliability Standard and applicable to all responsible entities in all circumstances. It is important that responsible entities have plans for introducing the personnel called in to assist in such situations. We expect that core training would be different for different responsible entities.

434. The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. 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. We note that, according to Requirement R1.4 of CIP-005-1, all cyber assets within an electronic security perimeter are to be protected, not just the critical cyber assets. In reply to commenters, we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee's duties, functions, experience, or access level. We agree with commenters that information concerning vulnerabilities should be revealed on a need to know basis and not universally. However, any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security.

435. Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves. Commenters provided minimal input on this proposal and, consistent with the CIP NOPR, we believe that whether a modification is appropriate to address this issue is better determined in the first

instance through the ERO's Reliability Standards development process. The ERO should consider the comments of SoCal Edison with regard to what role and steps should be taken by the ERO to ensure quality and consistency of trainers.

443. The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process. FirstEnergy and California Commission agree with the Commission's proposals.

444. ReliabilityFirst and SPP believe that it would be appropriate to handle emergency access via a short-term exception to the security policy. We note that such access would not be only an exception to the security policy, but an exception to a CIP Reliability Standard Requirement. Therefore, such exceptions would have to comply with the conditions of a technical feasibility exception that we have specified elsewhere in this Final Rule. The Commission believes that a workable solution is for the Reliability Standards development process to identify emergency circumstances that would warrant allowing access to critical cyber assets. However, if a responsible entity experienced a situation outside of those circumstances that it believed warranted access to critical cyber assets, the responsible entity could treat the situation as a technical feasibility exception and follow the conditions set out by the Commission. With this approach, we believe that in most cases it will be unnecessary to go through the administrative burden of a technical feasibility exception.

445. SoCal Edison expresses concern that the 30 days allowed in CIP-004-1 for completion of the personnel risk assessment may not be enough time to process all existing employees with access. We note that there is no reason why such assessments cannot be completed well before responsible entities are to be auditably compliant with this provision. The ERO should consider SoCal Edison's issue in the Reliability Standards development process.

446. APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process.

460. The Commission adopts the CIP NOPR proposal to direct the ERO to 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 physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

461. As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate. As noted in the CIP NOPR, most organizations will know in advance the timing of personnel actions and can arrange ahead of time for access revocation to be concurrent with any disciplinary action, transfer, retirement or termination. Revocation of access is usually a matter of assuring that a particular employee's credentials no longer permit physical or electronic access. We understand that outlying elements may require some brief lag before denial of access is effective, in which case, the circumstances justifying such lag must be documented for audit purposes.

462. FirstEnergy comments that the term “immediate” should be clarified and be interpreted as “as soon as possible” but not later than 24 hours to take care of on-the-spot dismissals. Others also comment about various circumstances where advance or coincident preparations for revocation to access cannot be made. We continue to believe that most dismissals can be anticipated in advance and believe that revocation should be immediate upon the employee’s notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible.

463. We acknowledge that not all disciplinary actions warrant revocation of access privileges. In addition, certain personnel transfers can require a protracted transitional process that warrants retention of access privileges after the formal transfer date. There may be operational reasons that justify retention of access privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes.

464. We also adopt our proposal to default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes. Our concern, in calling for this adjustment, is that the current language in the CIP Reliability Standard does not describe the purpose of the required list of personnel with authorized access; rather, it merely states that such a list must be made, reviewed, and updated. Similar to our expectations expressed earlier regarding implementation of required plans and policies, we believe that the expectation that access not be granted to personnel not on the authorized list should be made clear in the Reliability Standard. However, while a responsible entity should not allow access to any personnel not included on the list, the Commission believes commenters misunderstood the CIP NOPR and inappropriately linked the Commission’s proposal with respect to the immediate revocation of access with its proposal with respect to denying access to personnel not on the list. We clarify that we are not requiring the list to be updated simultaneously with the revocation of an employee’s access.

473. The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity’s obligations regarding vendors with access to critical cyber assets.

474. Regarding Northern Indiana’s comments, we do not believe that this Requirement obligates one joint owner of a critical cyber asset to perform risk assessments of another owner’s personnel. Each such owner is responsible for performing assessments of its own personnel.

475. The ERO should consider the suggestions raised by Northern Indiana, SPP and NRECA in the Reliability Standards development process. 476. Therefore, we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commission’s determinations above.

478. The Commission approves Standard CIP-005-1 as mandatory and enforceable.

496. The Commission adopts the CIP NOPR’s proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter. However, in light of the comments received, the Commission understands that there may be instances in which certain

facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. For that reason, the Commission believes that it is appropriate to allow the ERO and the Regional Entities to grant exceptions based on the technical feasibility of implementing defense in depth, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement electronic defense in depth measures or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

497. As stated in the CIP NOPR, the Commission recognizes that there is a point at which having multiple defense layers would not be cost effective. However, we continue to believe that the effectiveness of any one defense measure is often dependent on the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the protection of the Bulk-Power System. The Commission does not agree with Manitoba that providing one monitored and alarmed electronic security measure provides a sufficient and balanced security measure when implemented in conjunction with required physical security measures. A single electronic device is too easy to bypass and a physical security measure cannot thwart an electronic cyber attack. Therefore, we believe it is in the public interest to require that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter.

498. Many of the commenters' concerns with regard to the impact on performance and reliability will be alleviated by allowing Regional Entities to grant justified exceptions based on technical feasibility. For example, an exception might be granted if an entity can demonstrate that implementing any defense in depth mechanism would create a delay in the transmission of the data that is not tolerable on the system and cannot be mitigated. In addition, the Commission does not think that there will be a problem with respect to a delay in data transmission. If this is a problem for older or distant equipment, the responsible entity can claim a technical feasibility exception. Newer equipment should operate at sufficiently high speeds that multiple hops will not affect data transmission. In fact, some vendor companies claim that their devices will actually increase transmission speeds due to compression and other techniques.

499. Further, an exception might be granted until equipment is available for a given protocol or toolset used in a specific control system environment. However, the fact that additional equipment may take up space or use additional power and cooling alone does not warrant reversing the Commission proposal.

500. The Commission agrees with the ERO that requiring two or more defensive measures may increase the chance of equipment failure. But, the ERO has not provided the Commission with an adequate explanation of why the availability of the entire system would decrease with two or more defensive measures. Defensive measures can often be formatted so that if they fail, they do so in a fail-safe mode that still allows operation. Therefore, system availability would not decrease.

501. In response to SDG&E and Entergy, in stating that the placement of security measures in front of systems provides a layer of protection for those systems, the Commission was not giving priority to "in front" measures. In fact, the Commission acknowledged in the CIP NOPR that defense in depth measures are generally integrated within and constitute part of a system or program. In commenting that defense in depth measures may also be effectively placed in front of a system, the Commission intended only to acknowledge that there are multiple ways to implement a defense in depth strategy. The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity have at least two security measures unless it is not technically feasible to do so. The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment. The Commission believes that this, in conjunction with the allowance of technical feasibility exceptions, alleviates FPL Group's concern that the Commission's proposal is a "one size fits all" approach.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the **specific requirements should be developed in the Reliability Standards development process**. This would include whether or not the second security measure must be “on par” with the first. The Commission also **directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards**.

503. In response to Manitoba’s concern that the proposed additional security measure could delay implementation of the more important requirement of an electronic perimeter for all critical cyber assets, the Commission notes that this Final Rule approves the Reliability Standard as filed by the ERO. The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures. Until that Reliability Standard is developed by the ERO and approved by the Commission, responsible entities in the United States will not be required to implement two or more defensive measures.

504. The **ERO should consider in the Reliability Standards development process Northern Indiana’s and Xcel’s concerns regarding the phrase “single access point at the dial up device.”**

511. The Commission adopts the CIP NOPR’s proposal to **direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies**. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are **directing the ERO to provide guidance on what constitutes strong authentication**, it is not necessary for the Commission to respond to ISO-NE’s request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the **ERO should take into account the specific comments raised in this proceeding**. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, **we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption**. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

525. The Commission adopts the CIP NOPR proposal **to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects**. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily, as requested by Juniper.

526. The Commission agrees with MidAmerican that the review intervals should be designed to accomplish the detection and improvement objectives discussed in the CIP NOPR. **Requirement R3 of CIP-005-1 does not currently require a responsible entity to manually review logs if it has alerts**. However, the Commission continues to believe 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. Further, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs. The Commission believes allowing 90 days to pass without a log review is unacceptable. In that time, an incident could have occurred undetected or an attacker could have gained access to a critical system and extended that access throughout the enterprise with the targeted entity being unaware that the security of their systems had been compromised. For this reason, the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments. The Commission continues to believe that, in general, logs should be reviewed at least weekly, but leaves it to the Reliability Standards development process to determine the appropriate frequency. In addition, the Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.

527. In response to MidAmerican's concern about the term "bifurcated review," the Commission intent was that certain assets, deemed readily accessible, would be reviewed at least weekly while other assets would continue to be reviewed every 90 days. However, the Commission will not adopt this direction from the CIP NOPR. We leave it to the Reliability Standards development process to decide whether different timeframes are appropriate for logs that are readily accessible and not readily accessible. If different review timeframes are adopted, the ERO should provide guidance as to what constitutes a readily accessible log and a log that is not readily accessible. The ERO may also delineate different timeframes for manual review for other reasons, but must clearly define how to determine in what timeframe a specific log must be reviewed. However, we reiterate that any attempt to differentiate the required frequency of review of these logs must be balanced against the criticality of the facilities; it is not acceptable to dismiss a critical facility from timely review simply because it is remote.

528. Finally, the Commission also agrees with commenters that a full review of logs could be burdensome. Therefore, the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that the manner in which a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, any requirements for creating this sample review could be detailed in its cyber security policy so that it can be audited. The Reliability Standards development process should decide the degree to which the revised CIP-005-1 describes acceptable log sampling. The ERO could also provide additional guidance on creating the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the responsible entity to detect intrusions by attackers.

541. The Commission notes that the concerns expressed by some commenters of triggering an unknown vulnerability during a live test is one reason why some form of live or active testing is necessary. A responsible entity cannot protect its system from exploitation of vulnerabilities that it does not know about. However, in light of the comments received, the Commission will not adopt its proposal as set out in the CIP NOPR regarding live vulnerability assessments in Requirement R4 of CIP-005-1. Instead, we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments. Further, as discussed below, we clarify that an interim vulnerability assessment will only

need to be performed if a responsible entity makes a significant modification to the electronic security perimeter.

542. The Commission's goal in proposing live vulnerability testing is to provide a level of confidence that the Bulk-Power System has a certain level of resistance to attack. We understand the concerns raised by commenters that live vulnerability testing could, at this time, diminish reliability. While the Commission's goal is to require full live vulnerability testing on the entire Bulk-Power System at some point, we understand that this may not be possible at this time. As suggested by FirstEnergy, industry may need time to gain experience in this area before it can conduct full live vulnerability testing. Therefore, the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.

543. The Commission agrees with the ERO that test systems do not need to exactly match or mirror the operational system. However, to perform active vulnerability assessments, the responsible entities should be required to create a representative system, i.e., one that replicates the actual system as closely as possible. The active vulnerability assessment should be carried out on this representative system. In doing so, a responsible entity must document the differences between the operational and representative system for the auditors. As part of this documentation, the responsible entity should also document how test results on the representative system might differ from the operational system, and how the responsible entity accounts for such differences in operating the system. Our goal is to ensure that each responsible entity understands the differences between its representative system and the operational system and how those differences might affect its test results. The entities remain responsible, however, to ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

544. Further, the Commission agrees with commenters that requiring each responsible entity to perform a vulnerability assessment of the electronic access points when any modification is made to the electronic security perimeter or defense in depth strategy is too broad. Instead, the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification. To be clear, the Commission is not requiring the Reliability Standard to use the terminology that a "significant change" is made to the electronic security perimeter or defense in depth strategy. Rather, we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment. For example, we would anticipate that updating an attack signature file on the electronic access point would not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point would require an active vulnerability assessment.

545. Given our changes to the Commission proposal, and based upon the comments, the Commission does not believe performing an active vulnerability assessment once every three years will pose too great a burden on company personnel. The burden above that is required by the Reliability Standard as proposed by the ERO is justified by the insights that will be gained from the active assessments.

546. At this time, the Commission does not believe it is necessary to require twice a year penetration tests by responsible entities, as requested by Juniper. We believe that the combination of annual testing and active vulnerability assessments is sufficient for the Reliable Operation of the Bulk-Power System.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a

representative system and what modifications require an active vulnerability assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

559. We are persuaded by commenters that there may be instances in which the physical or safety-related obstacles to achieving a completely enclosed physical boundary cannot be overcome. In such instances, we agree with commenters that it would be inappropriate to treat the alternative measures under this CIP Reliability Standard as interim actions under the technical feasibility exception, as the exception was proposed in the CIP NOPR. However, the Commission has revised its determination with respect to the technical feasibility exception to address concerns such as those raised by commenters on Requirement R1.1 of CIP-006-1. The Commission believes that allowing a technical feasibility exception to Requirement R1.1 of CIP-006-1, with the changes discussed in the Technical Feasibility section of this Final Rule, should address commenters' concerns. Specifically, the Commission acknowledges that some circumstances merit reliance on mitigation strategies that are ongoing and effective, so long as they are justified and reviewed periodically. This should alleviate the concern of commenters that the Commission is not allowing exceptions to Requirement R1.1 on a long-term basis.

560. Therefore, the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions. In evaluating the requests for a technical feasibility exception to Requirement R1.1, we expect the ERO to work with the responsible entities to ensure consideration of any emerging technologies that may allow the responsible entity to satisfy Requirement R1.1.

572. The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets. However, similar to our determination in CIP-005-1 regarding defense in depth for electronic security perimeters, in light of the comments received, the Commission understands that there may be instances in which certain facilities cannot implement defense in depth or where such an approach would harm reliability rather than enhance it. For that reason, the Commission believes that it is appropriate to allow the ERO and the Regional Entities to grant exceptions based on the technical feasibility of implementing defense in depth, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement physical security perimeter defense in depth measures or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

573. As stated in the CIP NOPR, the Commission recognizes that there is a point at which implementing multiple layers of defense becomes an unreasonable burden to responsible entities. However, as more fully detailed in our discussion of defense in depth in CIP-005-1, we continue to believe that the effectiveness of any one defense measure is often dependent on the quality of active human maintenance, and there is no one perfect defense measure that will guarantee the protection of the Bulk-Power System. Therefore, we continue to require the use of layered and complementary security procedures that a defense in depth approach embodies.

574. In response to APPA/LPPC's comments, the Commission does not require two or more different monitoring methods under Requirement R3. We did not propose to modify Requirement R3 and are not doing so in this Final Rule. Further, the Commission did not intend to require two or more physical perimeters, as suggested by NERC and ReliabilityFirst. Rather, the Commission intended only to require

the ERO to modify R2 to provide for two or more different and complementary physical access controls at a physical access point of the perimeter. The Commission believes that this should clarify what it meant by the term “procedures” and sees no need to direct the ERO to define the term, as requested by Entergy.

575. In response to commenters’ questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complimentary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule. The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

576. Northern Indiana raises a concern about security measures in remote or field locations, but did not provide specific information. The Commission believes that, if it is not possible to implement two or more distinct physical security measures in a remote or field location, a Regional Entity could grant justified exceptions based on technical feasibility.

581. The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years, but clarifies our direction in several respects. Similar to our action with respect to reviewing logs in CIP-005-1, the Commission will not adopt the proposal to require different testing periods for physical security measures on critical cyber assets that are readily accessible or not readily accessible. Instead, we leave it to the Reliability Standards development process to decide whether different timeframes are appropriate for physical security measures on critical cyber assets that are readily accessible and not readily accessible. Similar to our direction in CIP-005-1, if different review timeframes are adopted, the ERO should provide guidance as to what constitutes a readily accessible facility and a facility that is not readily accessible. The ERO may also delineate different timeframes for testing for other reasons, but must clearly define how to determine in what timeframe the physical security measures on a specific critical cyber asset must be reviewed.

582. In response to Northern Indiana, the Commission does not believe it is necessary at this time to specify what would constitute a test, because each test may be different based on the type of physical security measure employed. Northern Indiana may ask the ERO to provide guidance on this matter.

583. In response to National Grid, we clarify that the CIP NOPR’s reference to the testing of critical cyber was inadvertent, and that we proposed testing intervals for physical security measures.

585. The Commission approves Reliability Standard CIP-007-1 as mandatory and enforceable.

597. The Commission affirms its proposals with respect to technical feasibility and acceptance of risk. Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2. However, as discussed in the CIP NOPR, this leaves intact the exception for technical limitations in Requirement R2.3, so long as the treatment of Requirement R2.3 conforms to our findings regarding the technical feasibility exceptions.

598. MidAmerican’s concerns about clarifying the terms technical limitations and technical feasibility through the Reliability Standards development process are addressed in our findings regarding technical feasibility elsewhere in the Final Rule.

599. In response to Juniper, the Commission does not believe that applying the technical feasibility exception in lieu of acceptance of risk means that a responsible entity would not have to mitigate the risk of not being able to turn off ports. The Commission believes that our discussion of the technical feasibility exception in the Technical Feasibility Exception Remediation and Mitigation section above supplies the obligation to mitigate that Juniper is seeking.

600. With respect to security patch management, the Commission continues to believe that the acceptance of risk language is unacceptable. However, in doing so we do not seek to prevent responsible entities from exercising some level of discretion. The Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility. The Commission believes that this will allow responsible entities the discretion APPA/LPPC seek. Further, this essentially accomplishes the outcome sought by MidAmerican. With respect to the disclaimer requested by APPA/LPPC, the Commission is not convinced to direct such a modification to the Reliability Standard at this time. However, this issue should be examined in the Reliability Standards development process. Given that we are modifying our direction, we do not believe that it is necessary to mandate senior management involvement in these decisions here. While we direct the ERO to modify Requirement R3 of CIP-007-1 to remove the acceptance of risk language, the ERO, through the Reliability Standards development process may choose to allow exceptions to this requirement for technical infeasibility, consistent with the Commission's determination on technical feasibility above. However, the responsible entity should implement the requirements for software patches for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to our discussion of technical feasibility exceptions.

609. The Commission has discussed issues related to testing environments in CIP-005- 1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a "representative system" – one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

610. Consistent with our action in CIP-005-1, the Commission will not at this time require documentation of each difference between the testing and the production environments and how each such difference is mitigated or otherwise addressed. In using the term mitigation, our goal was to ensure that each responsible entity understands the differences between its representative system and the production system and how those differences might affect its test results. The Commission believes that, as a part of this documentation, the responsible entity should also document how any test results might differ from the testing system to the production system and how the responsible entity accounts for such differences in operating the system. Therefore, we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above. Such revision should address what types of differences must be documented. The entities remain responsible, however, to ensure that the testing systems are adequate to model the production systems and to document and account for the differences between the two.

611. With respect to MidAmerican's proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO

should consider this matter in the Reliability Standards development process. However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.

612. The Commission understands Northern Indiana's concern that documenting vulnerability test results or any mitigation or remediation plans may reveal system vulnerabilities. The ERO should alleviate this concern by providing for such reports to be reviewed under the confidentiality provisions of its Rules of Procedure.

619. The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. Issues concerning technical feasibility and acceptance of risk are discussed above.

620. The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used. Further, as Consumers admits, any network infrastructure devices that are not directly targeted can be affected as collateral damage.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes how an entity should protect against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

622. Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

628. Requirement R6 of CIP-007-1 does not address the frequency with which logs should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1. Also, at this time, the Commission

does not believe that it is necessary to require responsible entities to maintain all logs for at least three years, as requested by Juniper.

629. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

630. In response to Northern Indiana, the Commission discusses our use of the term forensics in our discussion of CIP-009-1.

633. The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it. The Commission notes that there is a difference between redeploying an asset and discarding it. Redeploying an asset within the same responsible entity allows that responsible entity to maintain control over the asset, whereas disposing of an asset places it out of the control of the responsible entity. The Commission believes that, while the seven layer wipe described by Northern Indiana may be sufficient for redeployment because the responsible entity maintains control over the cyber asset, it is not sufficient for disposing of an asset.

634. The Commission disagrees with Northern Indiana that the only way to allow no opportunity to access data on storage media is to destroy the media. As stated in the CIP NOPR, high quality degaussing can adequately protect media from unauthorized access. [SRM1]Northern Indiana has not provided information that convinces the Commission that a cyber asset would have to be destroyed in order to prevent access.

635. Therefore, the Commission directs the ERO to revise Requirement R7 of CIP-007- 1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.

643. The Commission adopts its proposal to direct the ERO to 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.

644. The Commission agrees with ISO-NE that hardware and software is implemented in diverse ways throughout the industry, but does not believe that this renders providing guidance infeasible. We also agree that overly rigid guidance could result in responsible entities failing to properly test for vulnerabilities specific to the entities' environments and systems. The Commission does not believe that the revised Reliability Standard should be inflexible. It should encourage responsible entities to take into account emerging and diverse technologies and newly discovered vulnerabilities as they emerge. The Commission believes that it is appropriate to leave such guidance to the Reliability Standards development process. Further, we leave it to the ERO's discretion whether to put guidance in the revised Reliability Standard or a reference document.

645. The Commission addressed Northern Indiana's concerns about revealing vulnerability test results in our discussion of CIP-005-1. We believe that the ERO's confidentiality provisions should adequately protect against unwanted disclosure of vulnerability test results.

651. The Commission adopts a modified version of the CIP NOPR proposal. We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days. The Commission believes that 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation.

652. The Commission clarifies that the shorter period should begin upon final implementation of the modifications. The Commission believes that providing that the shorter period begins when the modifications are implemented satisfies Northern Indiana's concern about finalizing documentation and the potential need for internal reviews and approvals. By the time any modification is made, such approvals should already have been granted. Similarly, the Commission believes that MidAmerican's concern about resource constraints relate more to the implementation of a modification, not the documentation of that implementation. Once a modification is developed and implemented, documenting it should not consume significant time or resources.

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

661. Therefore, the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced.

673. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. As stated in the CIP NOPR, the reporting timeframe should run from the discovery of the incident by the responsible entity, and not the occurrence of the incident.

674. Most commenters are concerned with the burden placed on a responsible entity to report an incident when system restoration should take precedence. As stated in the CIP NOPR, while the Commission

agrees that, in the aftermath of a cyber attack, restoring the system is the utmost priority, we do not believe that sending this short report would be a time consuming distraction, and we judge that its probative value would justify the minimal time spent in making this report. In this respect, the Commission now clarifies that the responsible entity does not need to initially send a full report of the incident. Rather, to report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever useful preliminary information is available at the time. This could be accomplished by a phone call or another method. The responsible entity could then follow up with a full report once the system is restored.

675. With respect to the arguments by California Commission and Texas PUC concerning the term appropriate government authorities, we believe this determination should be made through the Reliability Standards development process.

676. Thus, the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report. The Reliability Standard development process should consider whether the ESISAC could act as an intermediary to promptly notify government authorities for responsible entities. While we expect the modified Reliability Standard to be consistent with our discussion above, we leave development of the details of how to report incidents while not burdening the recovery process to the Reliability Standards development process.

677. With respect to Entergy's question about the relationship between CIP-001-1 and CIP-008-1, the ERO should consider Entergy's concerns in the Reliability Standards development process. However, the Commission notes that, while CIP-001-1 requires the reporting of sabotage events, CIP-008-1 requires the reporting of all cyber security incidents. Not all cyber security incidents will be caused by sabotage, so not all incidents required to be reported under CIP-008-1 will be required to be reported under CIP-001-1.

686. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned. The Commission further directs the ERO to include language in CIP- 008-1 to require revisions to the incident response plan to address these lessons learned.

687. In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise.

689. The Commission approves Reliability Standard CIP-009-1 as mandatory and enforceable.

694. For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan. We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.

706. The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard. The Commission continues to believe that it is important to long-term reliability interests that responsible entities collect data in certain situations, such as immediately after system restoration or the recovery of critical cyber assets. In response to ISO-NE, the Commission does not believe that the requirement to keep log data contained in other CIP Reliability Standards is sufficient. As we stated in the CIP NOPR, the data collection procedures could include preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data. None of this is required in the Reliability Standards cited by ISO-NE.

707. The Commission used the term forensic because that is the term used in the Blackout Report. However, the Commission clarifies that it does not intend, as suggested by commenters, that the Reliability Standard impose the extent of scientific rigor or chain of custody required in criminal procedure. Rather, the Commission is concerned with responsible entities preserving the data necessary to determine the cause of any problem with the system.

708. In response to Entergy, NRECA, SoCal Edison and Northern Indiana, recovery of critical cyber assets and the Bulk-Power System is of immediate critical importance, and information collection efforts should not impede or restrict system restoration, as stated in the CIP NOPR. We agree that preserving evidence should not hinder system restoration.

709. We do not object to the alternate proposal developed by the ERO, including use of the phrase “data collection for post-event analysis, where technically feasible,” to describe what should be required under the revised Reliability Standard. The ERO may also consider the methods proposed by Entergy and MidAmerican. We also recognize that collecting forensic data may not be technically feasible for all situations due to equipment limitations, such as older substation installations with little electronic monitoring. Therefore, when revising the Reliability Standard, the ERO may incorporate a technical feasibility exception, subject to the same conditions for exercising the exception as described elsewhere in this Final Rule.

710. Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report. The modification should focus on responsible entities preserving the data necessary to determine the cause of any problem with the system and may include a technical feasibility exception.

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP-005-1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live

testing in CIP-005-1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this “demonstrated recovery” concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters’ concerns about the risks associated with such testing

726. The Commission notes ISO-NE’s concerns about providing a definition of full operational exercise in the NERC Glossary are addressed since we are not requiring the use of that term in the Reliability Standards.

731. The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans. We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective. As we stated with respect to change made pursuant to CIP-007-1, the Commission believes that having correct documentation is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could attempt to operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation. Northern Indiana has not provided us sufficient reason to change the CIP NOPR proposal. Finally, as stated with respect to the documentation requirements in CIP-007-1, the 30 day period should begin upon final implementation of the modifications.

739. The Commission adopts the CIP NOPR proposal to direct the ERO to modify 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. Our intent in doing so is to require responsible entities to have a procedure in place that gives them a high confidence level that their backups will actually restore the system as needed. Auditors should be able to determine compliance by reviewing a responsible entity’s policies, procedures and records to determine how the testing is done and what recent tests have been performed. In response to commenters’ suggestions on how to verify the backup and restoration processes, the ERO should determine appropriate methods to accomplish the Commission’s objectives in the Reliability Standards development process.

740. The Commission does not agree with FirstEnergy and Northern Indiana that requiring verification of backup and restoration processes and procedures when a significant change is made to the operational control system requires continuous assessment. The Commission does not believe that every change will necessitate verification of the backup and restoration processes. Rather, it is sufficient to verify a process if a significant change, such as adding new hardware or installing new software to the control system, is made. The Commission does not believe that responsible entities will be making significant changes to their backup and restoration processes continuously. Similar to our determination with respect to Requirement R4 of CIP-005- 1, the ERO should determine, through the Reliability Standards development process, what would constitute a modification that would require verification of the backup and restoration processes.

748. The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use. However, the

Commission agrees with ISO-NE that it is impractical to require the system to be shut down and be restarted with the data in order to test it. As stated above with respect to verifying backups after a significant change, our intent is to give responsible entities a high confidence level that their backups will actually restore the system as needed. Auditors should be able to look at a responsible entity's policies, procedures and records to determine how the testing is done and what recent tests have been performed. The ERO should determine appropriate methods to accomplish the Commission's objectives in the Reliability Standards development process.

757. NERC and other commenters ask the Commission to defer to NERC on the determination of Violation Risk Factors and allow NERC to reconsider the designations using the Reliability Standards development process. The Commission has previously determined that Violation Risk Factors are not a part of the Reliability Standards. In developing its Violation Risk Factor filing, NERC has had an opportunity to fully vet the CIP Violation Risk Factors through the Reliability Standards development process. The Commission believes that, for those Violation Risk Factors that do not comport with the Commission's previously-articulated guidelines for analyzing Violation Risk Factor designations, there is little benefit in once again allowing the Reliability Standards development process to reconsider a designation based on the Commission's concerns. Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations. NERC must submit a compliance filing with the revised Violation Risk Factors no later than 90 days before the date the relevant Reliability Standard becomes enforceable.

758. That being said, NERC may choose the procedural vehicle to change the Violation Risk Factors consistent with the Commission's directives. NERC may use the Reliability Standards development process, so long as it meets Commission-imposed deadlines. In this instance, the Commission sees no vital reason to direct the ERO to use section 1403 of its Rules of Procedure to revise the Violation Risk Factors below, so long as the revised Violation Risk Factors address the Commission's concerns and are filed no less than 90 days before the effective date of the relevant Reliability Standard. The Commission also notes that NERC should file Violation Severity Levels before the auditably compliant stage.

759. Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.

760. The Commission disagrees with Progress that the Commission's concerns with respect to the CIP Violation Risk Factors will result in overly conservative Violation Risk Factor assignments. We also disagree with the characterization that a Violation Risk Factor delineates the importance of the Reliability Standard. Rather, the Violation Risk Factors delineate the relative risk to the Bulk-Power System associated with the violation of each Requirement. The Commission believes that the analysis below appropriately takes into account the risk of violating each Requirement in the CIP Reliability Standards.

767. The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors. While the Commission hopes that APPA/LPPC are correct that there is not a substantial potential for assets to be overlooked, this is not a reason to not modify the Violation Risk Factors. As we stated in Order No. 672, the fundamental goal of mandatory, enforceable Reliability Standards and related enforcement programs is to promote behavior that supports and improves Bulk-Power System reliability. It is not imposing penalties. However, as APPA/LPPC recognize, overlooked assets could result in Bulk-Power System failure. This comports with the definition of a high Violation Risk Factor as a requirement that, if violated, could directly cause or contribute to Bulk-Power System instability, separation, or a cascading sequence of failures, or could place the Bulk-Power System at an unacceptable risk of

instability, separation, or cascading failures. APPA/LPPC have not provided a persuasive reason for the Commission to change its proposal to direct the ERO to modify the Violation Risk Factors.

768. Further, the Commission is not persuaded by the argument that the Violation Risk Factor should not be high because there is an incentive for responsible entities to proceed cautiously. The Violation Risk Factor should consider the risk to the system of noncompliance, regardless of other incentives that users, owners and operators of the Bulk- Power System have to comply.

769. Finally, the regional oversight over asset designation discussed by APPA/LPPC is not in place yet. Therefore, the Commission cannot rule on what it might be.

776. MidAmerican seems to misunderstand the purpose of the information collection statement. The OMB regulations require agencies to submit a burden estimate for collections of information contained in proposed rules, not for the entire cost of compliance. As stated in the CIP NOPR, the Commission only included the cost of developing the required documentation for the required policies, plans, programs and procedures in its burden estimate, but did not include in our burden estimate the cost of substantive compliance with the CIP Reliability Standards. MidAmerican raises concerns regarding the total cost of compliance with the Reliability Standards, rather than the burden associated with reporting requirements in the Reliability Standards. Therefore, the Commission does not believe it is necessary to revise the burden estimate based on MidAmerican's comments.

799. As of October 2007, there are 1,772 registered entities, of which the Commission estimates that approximately 1,400 will be responsible for compliance with the CIP Reliability Standards. Of these, the Commission estimates that the CIP Reliability Standards would apply to approximately 632 small entities, consisting of 12 small investor-owned utilities and 620 small municipal and cooperatives.

800. Arkansas Electric raises concerns with the cost to small entities of the modifications directed by the Commission. These modifications will be made by the ERO through the Reliability Standards development process. Until NERC files any revised Reliability Standards, the Commission cannot estimate their burden on any user, owner or operator of the Bulk-Power System, including small entities. The Commission therefore does not believe it is appropriate to speculate on the cost of compliance with any modified Reliability Standard at this time.

801. The Commission does not believe it is appropriate to grant California Cogeneration's request that NERC develop pro forma models of protocols and methodologies to be used by entities to facilitate compliance. As discussed in the section regarding guidance, that level of detail could potentially introduce common vulnerabilities resulting from all small entities implementing the Reliability Standards using a nearly identical solution. With respect to California Cogeneration's suggestion that NERC should have a formal role in collaborating to reduce compliance costs, the Commission will not direct that at this time. However, NERC should consider providing information to such groups. Further, the Commission believes that requiring the ERO to develop guidance on how to comply with the Reliability Standards should facilitate compliance by small entities.

802. The Commission also declines to direct the ERO to include a QF category in the Functional Model, as requested by Energy Producers. The Commission believes that this request is outside the scope of this rulemaking, which only concerns the CIP Reliability Standards proposed by NERC.

803. The Commission does not believe it is necessary to allow small entities a longer compliance timetable or to provide temporary waivers upon an adequate showing of work to attain compliance. As was stated in the CIP NOPR, the burden to small entities is not great, but the economic impact is justified as

necessary to protect cyber security assets that support Bulk-Power System reliability. Further, the Commission believes that allowing small entities to collectively select a single consultant to develop model software and programs to comply with the CIP Reliability Standard will allow the small entities to take advantage of any information known by larger entities or their consultants.

804. While Southwest TDUs are correct that the Commission acknowledges that the Reliability Standards could be made applicable down to the smallest entity, the Commission disagrees that this discounts the economic impact on these entities. As we stated in the CIP NOPR, to be included in the compliance registry, the ERO will have made a determination that a specific small entity has a material impact on the Bulk-Power System. A small entity placed on the compliance registry could then appeal the determination to the ERO and the Commission.

805. Further, Southwest TDUs argue that just because a larger entity is performing compliance does not mean the costs of compliance are not being passed on to the small entities. We agree; however, in allowing small entities to pool their resources and select a single consultant to develop model software and programs, each entity need not separately fund model software and programs development. Rather, that cost can be spread over several entities.

806. For the reasons stated in the CIP NOPR and above, the Commission certifies that this rule will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.