123 FERC ¶ 61,174
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Joseph T. Kelliher, Chairman;
Suedeen G. Kelly, Marc Spitzer,
Philip D. Moeller, and Jon Wellinghoff.

Mandatory Reliability Standards for Critical Infrastructure Protection — Docket No. RM06-22-001

ORDER DENYING REHEARING AND GRANTING CLARIFICATION

ORDER NO. 706-A

(Issued May 16, 2008)

1. On January 18, 2008, the Commission issued a Final Rule (Order No. 706)[1] approving, pursuant to section 215 of the Federal Power Act (FPA),[2] eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC). In addition, pursuant to section 215(d) of the FPA, the Commission directed NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission. In this order, we deny requests for rehearing and grant in part, and deny in part, requests for clarification, as discussed in the body of this order.

I. Background

2. On February 3, 2006, the Commission issued Order No. 672,[3] which established a process to select and certify an Electric Reliability Organization (ERO) and,

---

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040 (2008).

[2] 16 U.S.C. 824o (Supp. V 2005).

[3] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 71 FR 8662 (Feb. 17, 2006), FERC Stats. & Regs. ¶ 31,204 (2006), *order on reh'g*, Order No. 672-A, 71 FR 19814 (Apr. 18, 2006), FERC Stats. & Regs. ¶ 31,212 (2006).

subsequently, the Commission certified NERC as the ERO.[4] Pursuant to section 215 of the FPA, the ERO develops mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved by the Commission, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or the Commission can independently enforce Reliability Standards.[5]

3. On August 28, 2006, NERC submitted to the Commission for approval the following eight CIP Reliability Standards:

> **CIP-002-1 – Cyber Security – Critical Cyber Asset Identification**: Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.
>
> **CIP-003-1 – Cyber Security – Security Management Controls**: Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.
>
> **CIP-004-1 – Cyber Security – Personnel & Training**: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.
>
> **CIP-005-1 – Cyber Security – Electronic Security Perimeters**: Requires the identification and protection of electronic security perimeters and access points. The electronic security perimeters are to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002-1.
>
> **CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets**: Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

---

[4] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062 (ERO Certification Order), *order on reh'g & compliance*, 117 FERC ¶ 61,126 (ERO Rehearing Order) (2006).

[5] 16 U.S.C. 824o(e)(3) (Supp. V 2005).

CIP-007-1 – Cyber Security – Systems Security Management: Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

CIP-008-1 – Cyber Security – Incident Reporting and Response Planning: Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

4. The Commission, in Order No. 706, approved these eight CIP Reliability Standards as mandatory and enforceable. The Commission also approved NERC's proposed implementation plan and timetable and directed NERC to develop modifications to the CIP Reliability Standards pursuant to the NERC Reliability Standards development process to address specific concerns identified by the Commission.

II. Procedural Matters

5. The following entities filed timely requests for rehearing or clarification of Order No. 706: Edison Electric Institute (EEI), ISO/RTO Council, and MidAmerican Energy Company and PacifiCorp (collectively MidAmerican).

III. Discussion

A. NERC's Process for Developing Modifications to the CIP Reliability Standards and Developing Guidance Documents

1. Order No. 706

6. Order No. 706 directed NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission. The Commission stated that "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."[6]

7. In Order No. 706, the Commission also directed NERC to develop "guidance" in certain instances. The Commission explained that "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."[7] For example, the Commission directed NERC to provide guidance on the development of a risk-based assessment methodology pursuant to CIP-002-1.[8] The Commission also directed the ERO to develop guidance regarding other matters, including: (1) the topics and processes to be addressed in a cyber security policy required pursuant to CIP-003-1; and (2) the issues and concerns that a "mutual distrust" posture must address to protect a control system.[9]

2. Requests for Rehearing and Clarification

8. MidAmerican asks the Commission to clarify that all modifications and developments to the CIP Reliability Standards must be developed through NERC's American National Standards Institute (ANSI)-certified Reliability Standards development process. MidAmerican states that, without such clarification, modifications to the CIP Reliability Standards may not align with technical capabilities, or worse, may not provide the anticipated increase in reliability. MidAmerican states that the use of this process is necessary to assure that responsible entities will have the opportunity to participate in the Reliability Standards development process.

9. While EEI states that it generally agrees with the Commission's approach of directing the ERO to develop guidance for responsible entities on a number of topics related to the CIP Reliability Standards, it does not believe such guidance should be developed through the Reliability Standards development process. Therefore, EEI asks the Commission to modify Order No. 706 to direct the ERO *not* to use the NERC Reliability Standards development process to develop guidance and processes related to the implementation of the CIP Reliability Standards. EEI believes that the ERO should,

---

[6] Order No. 706 at P 30.

[7] *Id.* P 61.

[8] *Id.* P 253. The Commission stated that the ERO had the discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.

[9] *Id.* P 355, 407-12.

instead, use an alternative open and transparent stakeholder procedure to develop such guidance. According to EEI, the NERC Reliability Standards development process should be avoided for the development of guidance because it requires approval by the NERC Board of Trustees, which is not necessary for a guidance document. Further, EEI suggests that the formal process is not well structured to timely update guidance in response to new situations and issues.

10. Similarly, while EEI states that it supports the Commission's finding that the ERO should provide written guidance to assist entities to develop an adequate risk-based assessment methodology pursuant to CIP-002-1, it seeks clarification on several aspects of this determination. Again, EEI urges that the ERO not use the Reliability Standards development process to develop such guidance but, rather, asks that another open and transparent stakeholder process be used. It also asks the Commission to clarify that the decision of whether to incorporate such guidance into the CIP Reliability Standards is a matter to be determined in the Reliability Standards development process, and not left to the ERO's discretion.

11. EEI also asks the Commission to clarify that guidance provided by the ERO serves as a resource and guide for responsible entities but is not binding or subject to enforcement as a Reliability Standard.

3. Commission Determination

12. In response to MidAmerican, the Commission has been clear that any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and vetted through NERC's ANSI-certified Reliability Standard development process.[10]

13. In Order No. 706, the Commission directed the ERO to provide sufficient guidance in certain instances to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. We stated that more guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Therefore, in several instances throughout Order No. 706, the Commission directed the ERO to provide additional guidance. In some cases, Order No. 706 specifically left it to the ERO's discretion whether to incorporate such guidance directly into the CIP

[10] *See id.* P 30; Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, Stats. & Regs. ¶ 31,242, at P 187 (2007).

Reliability Standard, incorporate the guidance into a separate reference document, or some combination of the two.[11]

14. The Commission denies EEI's request for clarification regarding the ERO's development of guidance. The Commission leaves to the ERO's discretion the appropriate procedure for the development of such guidance, including guidance to assist entities to develop an adequate risk-based assessment methodology pursuant to CIP-002-1. Of course, if the ERO determines that any such guidance should be incorporated into a CIP Reliability Standard, any such modification of the Reliability Standard must be developed pursuant to the ERO's Reliability Standards development process.

15. The Commission agrees with EEI that there is an important distinction between a Reliability Standard and a guidance document. While a Reliability Standard sets forth mandatory and enforceable compliance obligations, a guidance document should provide valuable assistance to responsible entities on how to achieve compliance with the requirements of a Reliability Standard. A guidance document, however, is not binding and cannot be the subject of an enforcement action, unless it is incorporated into a Reliability Standard.

B. Technical Feasibility

1. Order No. 706

16. In Order No. 706, the Commission noted that several CIP Reliability Standards provide exceptions from compliance based on "technical feasibility." While the Commission did not object to a technical feasibility exception, it recognized the need to provide control and oversight when an entity invokes the exception. While the final rule found it unnecessary to direct NERC to define technical feasibility in its glossary, the Commission directed 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.[12]

17. In discussing the set of conditions or criteria for granting a technical feasibility exception, the Commission acknowledged that, 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

[11] *Id.* P 61.

[12] Order No. 706 at P 178.

measures are not possible, the possibility of being required to replace equipment before the end of its useful life is a valid concern.[13]

18. The Commission did not require pre-approval of a claimed technical feasibility exception. Rather, the Commission stated that Regional Entities should, in the first instance, receive and catalogue notices of technical feasibility exceptions that are claimed. We stated that such notices must include an estimate of the degree to which mitigation measures achieve the goals set by a CIP Reliability Standard and provide 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. Further, Order No. 706 provided that actual evaluation and approval of technical feasibility exceptions should be performed in the first instance in the audit process.[14]

2. Requests for Rehearing and Clarification

19. MidAmerican states that the term "technical feasibility" remains "ill-defined" and seeks clarification or a finding on rehearing that entities will have an opportunity to participate in the process of defining "technical feasibility." It contends that any hint of ambiguity could result in confusion and delays.

20. While EEI states that it supports the Commission finding that Regional Entities should, in the first instance, receive and catalogue notices of technical feasibility exceptions that are claimed, EEI asks the Commission to clarify that the ERO should ensure that Regional Entities are consistent in conducting these activities. EEI asks that the Commission direct NERC to develop a uniform procedure to ensure consistency by Regional Entities in processing notices of technical feasibility exceptions. EEI also requests that the Commission direct the ERO to make clear that the provisions on confidentiality in section 1500 of NERC's Rules of Procedure will apply to the Regional Entities when handling information related to a responsible entity's invocation of the technical feasibility exception.[15]

21. EEI also asks for clarification that cost considerations can support invoking the technical feasibility exception. EEI states that although the Commission concluded that cost can be a valid consideration, EEI is concerned that the Commission appears to only address concerns about costs related to "legacy equipment." It notes that, while the

---

[13] *Id*. at P 180, 193-194.

[14] *Id.* P 213.

[15] EEI Rehearing Request at 17.

Commission concluded that technical feasibility should be interpreted narrowly to not include considerations of business judgment, the Commission stated elsewhere that the absence of references to reasonable business judgment will not prevent cost consideration from happening.[16] EEI also points out that the Commission acknowledged that resources for cyber protection are not infinite and that cost is a relevant consideration for looking at replacing long-life legacy equipment. Further, according to EEI, without clarity that cost considerations are legitimate in invoking the technical feasibility exception, entities may be unnecessarily encouraged to obtain cost-prohibitive controls that do not add value in terms of security.

22. Finally, EEI asks the Commission to clarify that it is solely the responsible entity's decision, subject to audit, whether and when equipment is at the end of its useful life. EEI argues that the responsible entity is in the best position to evaluate whether "equipment is near the end of its useful life or if insufficient mitigation measures are available."[17]

3. Commission Determination

23. The Commission denies MidAmerican's request that the Commission direct the ERO to define the term technical feasibility. MidAmerican has not provided the Commission with any specific concern regarding its assertion that the definition of technical feasibility is ambiguous. As the Commission stated in Order No. 706, 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.[18] Because technical feasibility determinations require case-by-case analysis, there may not be one concise definition that can be applied for all situations. For this reason, the Commission continues to believe that 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.

24. As to EEI's request for clarification regarding consistency in processing technical feasibility exceptions, we expect Regional Entities to process and evaluate requests for technical feasibility on a fair and consistent basis. However, we will not direct that the ERO and Regional Entities develop a specific procedure to ensure uniformity. Rather, we leave to the discretion of the ERO whether the development of a uniform procedure,

---

[16] *Id.* at 15, *citing* Order No. 706 at P 132, 186.

[17] *Id.* at 16, *citing* Order No. 706 at P 194.

[18] *Id.*

such as a revision to the NERC Rules of Procedure, is appropriate to provide the expected level of consistency in processing technical feasibility exceptions.

25. With regard to EEI's confidentiality issue, the Commission notes that section 1500 of NERC's Rules of Procedure requires "a receiving entity [to] keep in confidence and not copy, disclose, or distribute any confidential information or any part thereof without the permission of the submitting entity, except as otherwise legally required."[19] Section 1502 of NERC's Rules of Procedure defines a receiving entity as either the ERO or a Regional Entity. Therefore, to the extent that information collected on claimed technical feasibility exceptions meets the definition of confidential information, section 1500 would require both the ERO and the Regional Entity to keep such information confidential. However, the ERO should consider whether section 1500 is the appropriate safeguard for keeping technical feasibility information confidential or if such information should be protected another way.

26. With respect to EEI's request for clarification that cost considerations can support a technical feasibility exception, the Commission believes that this determination must be made on a case-by-case basis. The Commission did not intend to only address cost concerns with legacy equipment. We acknowledged 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.[20] While we stated that 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. We reiterate that these determinations must be made on a case-by-case basis. The ERO or a Regional Entity will need to approve any technical feasibility exception based on a claim that the equipment is not near the end of its useful life, taking into account whether the technical feasibility exception is needed and whether the mitigation and remediation steps are adequate to the circumstance. Further, the Commission did not assume that technical infeasibility issues would be present only during the transition period, nor did it assume that on a going-forward basis there would be only one single means to comply with the CIP Reliability Standards.

27. However, with respect to cost considerations, the Commission reiterates that all responsible entities eventually must achieve full compliance with the CIP Reliability Standards when the equipment that creates the need for the exception is supplemented,

---

[19] NERC Rules of Procedure, § 1502.2.

[20] Order No. 706 at P 180.

upgraded or replaced. As such, we continue to believe that technical feasibility exceptions should not be necessary for future assets.[21]

28. Finally, EEI asks the Commission to clarify that, in the first instance, it is the responsible entity's sole decision whether and when equipment is at the end of its useful life. The Commission disagrees that it is the responsible entity's "sole" decision. As recognized by EEI, the responsible entity's determination is subject to audit, i.e., it is subject to the conditions on claiming a technical feasibility exception laid out in Order No. 706.

C. CIP-002-1 Critical Cyber Asset Identification

29. Reliability Standard CIP-002-1 addresses the identification of critical cyber assets.[22] Pursuant to CIP-002-1, a responsible entity must develop a risk-based assessment methodology to use in identifying its critical assets.[23] Requirement R1 specifies certain types of assets that an assessment must consider for critical asset status and also allows the consideration of additional assets that the responsible entity deems appropriate. Requirement R2 requires the responsible entity to develop a list of critical assets based on an annual application of the risk-based assessment methodology. Requirement R3 provides that the responsible entity must use the list of critical assets to develop a list of associated critical cyber assets that are essential to the operation of the critical assets.

30. The Commission, in Order No. 706, approved CIP-002-1. The Commission directed the ERO to provide additional written guidance regarding the development of a risk-based assessment methodology to identify critical assets. The Commission also directed that either the ERO or its designee provide reasonable technical support to assist certain entities in determining whether their assets are critical to the reliability of the Bulk-Power System.[24] Order No. 706 also recognized the need for external oversight of

---

[21] *Id*. P 181.

[22] The NERC Glossary defines "cyber assets" as "programmable electronic devices and communication networks including hardware, software, and data." It defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets."

[23] NERC defines "critical assets" as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

[24] Order No. 706 at P 255.

critical asset identification to provide a regional perspective and for the ERO to develop, pursuant to the Reliability Standards development process, a mechanism for external review and approval of critical asset lists.[25] The Commission left to the discretion of the ERO whether the Regional Entity should conduct the external reviews or whether another entity, such as the reliability coordinator, should conduct the reviews with Regional Entity oversight.[26]

1. Technical Support on Risk-Based Assessment Methodology

a. Order No. 706

31. As mentioned above, the Commission directed the ERO or its designees to provide both additional written general guidance regarding the development of a risk-based assessment methodology to identify critical assets[27] and reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical.[28] The Commission, in Order No. 706 explained that, "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."[29] The Commission, therefore, allowed the ERO the discretion to designate another type of entity with a wide-area view, such as the reliability coordinator, to provide needed assistance.

b. Requests for Clarification or Rehearing

32. EEI asks the Commission to clarify that any responsible entity that lacks a wide-area view or for other reasons requires guidance on developing its risk-based assessment methodology may request technical assistance, regardless of its size. EEI also requests clarification that the ERO or its designee will provide such assistance only upon request. EEI also contends that it is not appropriate for the ERO or Regional Entities to provide unsolicited technical assistance. According to EEI, any guidance provided as part of this technical assistance should be non-binding.

---

[25] *Id.* P 322.

[26] *Id.* P 327-28.

[27] *Id.* P 253-54.

[28] Id. P 255.

[29] *Id.*

c. Commission Determination

33. In Order No. 706, the Commission adopted the NOPR proposal that the ERO and Regional Entities should provide reasonable technical support to relatively smaller entities, "to assist [such] entities in determining whether their assets are critical to the Bulk-Power System."[30] At the same time, we did not require that technical assistance be extended to all responsible entities, because we were "mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities."[31]

34. While we continue to find that smaller entities should receive needed technical assistance, we will not require the ERO and Regional Entities to provide technical assistance to all responsible entities which are engaged in developing a risk-based methodology. The ERO or its designee may provide technical assistance on a limited basis, at its discretion, if it believes it has the capability to do so. As indicated in Order No. 706, it is anticipated that certain entities may have difficulty determining whether a particular asset is critical because that entity lacks a wide-area view.[32] For example, the impact of a facility may be dependent on a connection with a transmission owner or operator. For such entities, the ERO or its designee should provide technical assistance. To the extent necessary, we leave to the discretion of the ERO to provide further refinement of the types of entities eligible for such assistance.

35. Further, the Commission agrees with EEI that technical assistance regarding risk-based assessments should only be provided at the request of the registered entity. Any concerns of the ERO or its designee regarding an entity's risk-based assessment would more appropriately be addressed in the external review process or a compliance action, and should not be expressed in the form of unsolicited technical advice. We also agree that technical assistance in performing a risk-based assessment is just that, and is not binding on the entity that requests it. The responsibility for properly performing a risk-based assessment rests firmly with the responsible entity. The fact that the Commission has directed the ERO to provide reasonable technical support does not shift this responsibility from the responsible entity to whatever entity provides the technical support. Finally, we note that the ERO may issue unsolicited clarifying instructions to industry at any time to ensure consistency and/or compliance based on its or its designee's review of the implementation of the Reliability Standards.

---

[30] *Id.*

[31] *Id.*

[32] *Id.*

2. Disputes Over Assets Added to a Critical Asset List

a. Order No. 706

36. In directing that the ERO develop a mechanism for external review and approval of critical asset lists, the Commission explained 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."[33] Further, the Commission recognized that there may be a legitimate need for a responsible entity to dispute such a determination and left to the discretion of the ERO whether there is a need for an appeal mechanism and, if appropriate, the development of appeal procedures.

b. Requests for Clarification or Rehearing

37. EEI makes several requests regarding this issue. EEI contends that the requirement of a pre-audit review and approval process demands that there be an appeals process. Thus, EEI states that the Commission should modify Order No. 706 to direct the ERO to develop appeals procedures, or to require that the existing appeals procedures set forth in the ERO's Rules of Procedure will apply in disputes between a responsible entity and an external reviewer regarding whether to identify an asset as critical.

38. Further, EEI states that, given the costs and resources required to protect additional assets, the Commission should clarify that implementation of any recommended changes directed by a third-party reviewer should be stayed during any appeal process. EEI states that this approach is needed to assure that an appeal is meaningful and consistent with due process principles. According to EEI, allowing the responsible entity to complete the appeal process before implementing an external reviewer's directive is consistent with NERC's treatment of remedial action directives.[34]

39. Finally, EEI disagrees with the Commission's determination 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.[35] According to EEI, if a responsible entity can reasonably explain its asset determination, there should be a presumption that this is the correct choice. It claims that, in many instances, it is likely that the external reviewer's technical expertise will not exceed that of the responsible entity, which has the best knowledge of its own environment and systems.

---

[33] Order No. 706 at P 325.

[34] EEI Rehearing Request at 18, *citing* CMEP sections 1.1.18 and 7.0.

[35] *Id.* at 18, quoting Order No. 706 at P 325.

c. Commission Determination

40. The Commission denies EEI's request and affirms that the external reviewer should prevail in a dispute over whether to include an additional asset to the critical asset list.[36] The Commission's overriding concern is to ensure that all critical assets are identified and protected. Thus, if there is a dispute as to whether an asset should be included in a responsible entity's list of critical assets, the default position should be to include the asset.

41. The ERO has not developed its process for external review. The Commission, therefore, believes that it is premature to determine whether that process must include an appeals mechanism. In the first instance, EEI will have an opportunity to raise any concerns it may have about the need for an appeals mechanism when the ERO develops its external review process. Further, entities will have the opportunity to raise concerns when the ERO submits this process for approval.

42. EEI also requests clarification that, where an external reviewer identifies an additional asset that should be included in a critical asset list, implementation should be stayed during an appeals process. Again, the Commission believes that it is premature to address this issue when the ERO has not developed its external review process. As a general matter, the Commission disagrees that an appeals mechanism developed by the ERO must provide an automatic stay. However, it may be appropriate to allow a stay on a case-by-case basis as determined by the ERO.

3. Confidentiality

a. Order No. 706

43. The Commission, in Order No. 706, recognized that critical asset lists likely contain sensitive information that needs to be protected from public dissemination.[37] Thus, the Commission stated that adequate safeguards need to be developed to assure that the information contained in critical asset lists is not released during the external review. Order No. 706 provided that the ERO, in developing an appropriate external review mechanism, should include features for the controlled delivery of critical asset lists to the external reviewer and identify minimum safeguards for the external reviewer to employ. The Commission also agreed with commenters that the external reviewer should not become a "central repository" for critical asset lists, and that such information should be returned to the responsible entity once the review is complete.

---

[36] *See* Order No. 706 at P 325.

[37] *Id.* at P 330-31.

b. Requests for Clarification or Rehearing

44. EEI agrees that the ERO should identify minimum safeguards and asks the Commission to clarify that the ERO should develop, with stakeholder input, an on-site review option that can be exercised by a responsible entity. EEI contends that allowing for on-site review of critical asset lists is likely more secure than a "controlled delivery" of critical asset lists to the external reviewer, would avoid costs associated with controlled delivery, and would avoid making the external reviewer a central repository of sensitive information. EEI also asks the Commission to clarify that the external reviewer must comply with applicable CIP Reliability Standards, including the training and background checks required by CIP-004-1.

c. Commission Determination

45. The Commission will not direct the ERO to develop an on-site review option that can be exercised by the responsibility entity, as requested by EEI. As described by EEI, such an option would be compulsory on the external reviewer when requested by the responsibility entity. While on-site review does have security benefits, it is also potentially extremely burdensome. While we are mindful of the need to maintain the confidentiality of information regarding critical asset lists, other means to secure this information are available. Thus, we will not direct an on-site review option.

46. In addition, while an external reviewer may not be an applicable entity under certain CIP Reliability Standards, we would expect that the safeguards developed by the ERO to assure that the information contained in a critical asset list is not released during an external review would include training and background checks, similar to those required in CIP-004-1.

4. Role of Reliability Coordinators in External Review

a. Order No. 706

47. While Order No. 706 provided that the Regional Entities must have a role in the external review of critical assets to assure that there is sufficient accountability in the process,[38] it left to the ERO to determine whether the Regional Entities have, or can timely develop, the resources to conduct the external reviews.[39] Alternatively, the Commission stated that the ERO may determine that another entity may be best equipped to conduct the reviews. While the Commission noted that commenters made a strong

[38] *Id.* P 327.

[39] *Id.* P 328.

case that reliability coordinators are the appropriate entity to perform the reviews, the Commission found that ERO should decide the best approach with its understanding of the capabilities and limitations of the Regional Entities.

b. Request for Clarification or Rehearing

48. ISO/RTO Council seeks confirmation that a reliability coordinator's potential involvement in the review of critical assets would not extend to the review of critical cyber assets.[40] ISO/RTO Council states that a reliability coordinator could offer expertise with respect to "physical" critical assets, but has no particular expertise in identifying critical cyber assets. Related, ISO/RTO Council seeks clarification that the potential role of a reliability coordinator would extend only to "fielded" generation and transmission assets, and not to control centers. It explains that the risk and impact of a control center is predominately cyber-oriented and, therefore, the reliability coordinator would not be the most appropriate reviewer.

49. ISO/RTO Council notes that Order No. 706 gave Regional Entities primary responsibility for oversight of a responsible entity's critical asset list, but gave NERC discretion to assign this oversight function to another entity such as reliability coordinators. ISO/RTO Council maintains that, if NERC designates reliability coordinators to perform this external oversight role, the reliability coordinators are in effect being asked to take on a duty that Regional Entities would normally undertake if they had the technical expertise or resources to do so. Based on these concerns, ISO/RTO Council asks the Commission to clarify that reliability coordinators should receive compensation if they, and not Regional Entities, are selected to perform the reviews. In addition, ISO/RTO Council asks the Commission to clarify that a reliability coordinator should be given the same liability protections afforded to a Regional Entity that conducts such a review, if it is later determined that a user, owner or operator failed to properly identify an asset as a critical asset.[41]

c. Commission Determination

50. The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets. The responsible entity is in the best position to

---

[40] ISO/RTO Council Rehearing Request at 5-6, citing Order No. 706 at P 324.

[41] *Id.* at 7-8 & n.16. ISO/RTO Council notes that the *pro forma* delegation agreement states that a Regional Entity has no liability to NERC regarding its performance of its responsibilities except in cases of gross negligence or willful misconduct.

make the initial identification of the critical cyber assets associated with the critical assets identified in its assessment. Moreover, while the external reviewer would add an important perspective to the identification of critical assets, it would not have the intimate knowledge of the responsible entity's control system that the responsible entity would have, and it would be less productive for the external reviewer to spend time reviewing the responsible entity's identification of critical cyber assets. Nevertheless, we caution that a responsible entity's identification of critical cyber assets needs to be designed to provide the same level of objectivity that would be provided by a third party's review. We also agree with the ISO/RTO Council that oversight of a responsible entity's identification of critical cyber assets would occur at the compliance audit stage. In addition, other compliance mechanisms such as spot checks or self-certifications could be appropriate means to address the completeness of a responsible entity's identification of critical cyber assets.

51. In response to ISO/RTO Council's concern regarding control centers, Order No. 706 stated that "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."[42] A responsible entity's decision to exclude the control center from its critical asset list must be subject to the external review. The Commission will leave to the ERO's discretion how to best accomplish such review, since the ERO has not yet determined whether the reliability coordinators will play a role in the external review of critical asset lists. The Commission denies ISO/RTO Council's request for clarification on this point. ISO/RTO Council should, rather, raise its concerns with the ERO in its development of the external review process. We note, however, that it would be the nature of the "physical" assets controlled by a control center that dictates designating the control center as a critical asset, and it would not be driven by the cyber-oriented impact as suggested by ISO/RTO Council.

52. As to ISO/RTO Council's argument that reliability coordinators or other entities designated by the ERO should receive compensation if they, and not Regional Entities, are selected to perform reviews of a responsible entity's critical assets, we do not believe that we should dictate how the parties resolve questions about the funding of such reviews. Instead, we will leave this to the parties involved to work out.

53. Moreover, we agree that entities designated by the ERO to perform reviews of a responsible entity's critical asset list should receive the same liability protection for performing this review that the ERO or Regional Entity would have if it performs this review itself. The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly

[42] Order No. 706 at P 280.

with the responsible entity. The fact that the Commission has directed the ERO to develop an external review process -- as a backup to help assure that the responsible entity does not overlook any critical assets -- does not shift this responsibility from the responsible entity to whatever entity conducts the external review.

5. Compliance Schedule for Newly-Identified Critical Assets

a. Request for Clarification or Rehearing

54. EEI states that, although raised by commenters, Order No. 706 did not address the schedule for how a responsible entity must bring a newly identified critical asset and its associated critical cyber assets into compliance. EEI states that, while not expected to change frequently, a critical asset list may change for legitimate reasons. EEI argues that, in such a case, the responsible entity needs an appropriate period of time to achieve compliance. Currently, however, there is no process or guidance on this issue. Thus, EEI requests that the Commission grant rehearing and direct the ERO to develop, through the Reliability Standards development process, a process for bringing newly identified critical assets into compliance. EEI states that such a process will encourage responsible entities to maintain critical asset lists that reflect current conditions.

b. Commission Determination

55. The Commission denies EEI's request for rehearing on this issue but, rather, provides the following clarification. Order No. 706 approved NERC's proposed implementation plan and its schedule and time frames for responsible entities to achieve compliance. In addition, the Commission directed the ERO to submit a work plan for developing modifications to the Reliability Standards and to submit this plan to the Commission for approval.[43] In addition, the Commission directed the ERO to consider making its modifications to CIP-002-1 and developing provisions regarding technical feasibility exceptions its first priority. We also stated that we would consider a second implementation plan for achieving compliance with the revised CIP Reliability Standards. Since these revised CIP Reliability Standards could cause additional critical assets to be identified through the external review process, the Commission expects that the second implementation plan would include the compliance timetable for newly identified critical assets.

56. We note that the NERC implementation plan that we approved in Order No. 706 contains a compliance schedule for Reliability Standards CIP-002-1 through CIP-009-1

[43] *Id.* P 89.

for entities registering in 2007 and thereafter,[44] and we expect that when NERC develops a schedule for responsible entities to bring newly identified critical assets into compliance with Reliability Standards CIP-002-1 through CIP-009-1, this schedule would be at least as prompt as the schedule it proposed in Table 4 of its Implementation Plan for compliance by newly registered entities.

D. CIP-004-1 Personnel and Training -- Revocation of Access to Critical Cyber Assets

1. Order No. 706

57. In Order No. 706, the Commission directed the ERO to develop modifications to Reliability Standard 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.[45] Order No. 706 explained that most organizations will know in advance when personnel actions will be taken and can arrange ahead of time for access to be revoked concurrent with any disciplinary action, transfer, retirement or termination. Further, the Commission stated that "[w]e understand that outlying elements may require some brief lag before denial of access is effective, in which case, the circumstance justifying such lag must be documented for audit purposes."[46]

2. Request for Clarification or Rehearing

58. EEI requests rehearing of the Commission's determination to require "immediate revocation" of access privileges. EEI maintains that the Commission erred in holding that revocations should be "immediate" or even "simultaneous," since this is not possible in most cases, and the Commission has not established any evidence in the record to support its assertion that "most dismissals can be anticipated in advance." Moreover, EEI argues that, even when dismissals are known in advance, this standard may not be achievable. Furthermore, the Commission has recognized that access to protected information should cease "as soon as possible but no later than 24 hours from the time of

[44] NERC Implementation Plan, Table 4. Table 4 provides the timetable for newly registered entities. While this table does not govern previously registered entities that identify additional assets in their external review, we believe that adding an additional asset should be accomplished at least as promptly as bringing a newly registered entity into compliance.

[45] *Id.* P 460.

[46] *Id.* P 461.

termination for cause." Consistent with this reasoning, EEI asks the Commission to modify Order No. 706 to require the ERO to develop a modification to CIP-004-1 to require revocation of access to be completed as soon as possible but not later than 24 hours from the time the employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason.

59. If the Commission declines to modify Order No. 706 with respect to "immediate" revocation of access privileges, EEI asks the Commission to modify Order No. 706 to direct the ERO, through the Reliability Standards development process, to define the circumstances that justify an exception to "immediate" revocations, and to determine a reasonable amount of time for such revocations of access to be completed. According to EEI, this clarification is consistent with the Commission's acknowledgment that "[t]here may be operational reasons that justify retention of access privileges after an employee transfers."[47]

3. Commission Determination

60. The Commission denies EEI's request for rehearing. While we do not dispute EEI's contention that there may be instances where the need for revocation cannot be anticipated in advance, or instances where revocation cannot be accomplished immediately, we addressed these concerns in Order No. 706 by allowing the ERO to provide for exceptions to the general policy requiring immediate revocation.[48] This marked a departure from the original proposal in the CIP Assessment in recognition of concerns that immediate revocation would not be possible in all instances. Thus, while we continue to believe that most dismissals can be anticipated in advance, and that a general rule providing for immediate revocations provides the best protection against security risks by disgruntled former employees and others, we also reaffirm our determination in Order No. 706 that the ERO should be given discretion to define the circumstances that justify an exception to immediate revocation, and to determine a reasonable amount of time for such revocations of access to be completed.

61. The Commission declines to require the ERO to define the criteria to justify exceptions to the immediate revocation Requirement. While Order No. 706 allowed the ERO to define what circumstances justify an exception to the immediate revocation Requirement, it did not require the ERO to do so. However, because the Commission directed the ERO to modify CIP-004-1 to require immediate revocation of access privileges, any exception to that Requirement should also be in the Reliability Standard. Therefore, should the ERO decide that exceptions to the immediate revocation

[47] *See* EEI Rehearing Request at 20, citing Order No. 706 at P 463.

[48] Order No. 706 at P 462.

Requirement are warranted, the ERO must use the Reliability Standards development process to develop both the Requirement and exceptions to the Requirement. If EEI believes that the ERO should "define what circumstances justify an exception that is other than immediate" it should raise its concerns in the Reliability Standards development process.

E. CIP-005-1 – Electronic Security Perimeter(s)

62. The Commission approved Reliability Standard CIP-005-1, which requires identification and protection of the electronic security perimeters within which all critical cyber assets are located, as well as all access points. In addition, we directed the ERO to develop modifications to this CIP Reliability Standard and required the ERO to clarify and provide guidance on other matters.

1. Requirement for Two or More Defensive Measures

a. Order No. 706

63. In Order No. 706, the Commission directed 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.[49] The Commission acknowledged 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 and allowed 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.

64. While the Commission recognized that there is a point at which having multiple defense layers would not be cost effective, we stated 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. We stated that a single electronic device could more easily be bypassed than multiple safeguards and that a physical security measure cannot thwart an electronic cyber attack.

[49] Order No. 706 at P 496-500.

b. Requests for Clarification or Rehearing

65. MidAmerican requests rehearing of the Commission's directive that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter. MidAmerican states that it is concerned that this requirement may not properly account for those circumstances in which a single device with multiple interfaces or forms of control may provide sufficient defense in depth without requiring more than one physical device. MidAmerican therefore requests that the Commission clarify whether two or more distinct physical devices must be installed to meet the "two or more distinct security measures" requirement, and if so, whether the two or more devices may be of the same type or make. MidAmerican requests that the Commission clarify, or find on rehearing, that responsible entities may determine the number of physical devices necessary as long as the goal of defense in depth achieved by the recommended "two or more distinct security measures" is met. According to MidAmerican, granting such a clarification would be a reasonable accommodation for those cases where requiring additional physical devices may add complexity and introduce additional risk not necessary to meet the technical objectives of layered security.

c. Commission Determination

66. The Commission denies MidAmerican's request for rehearing. As stated in Order No. 706, we directed the ERO to develop a requirement that each responsible entity must implement two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter.[50] To meet this requirement, Order No. 706 stated that it is in the public interest to require a responsible entity to implement "two or more *distinct* security measures when constructing an electronic security perimeter."[51] The Commission believes that a responsible entity cannot meet the goal of defense in depth as required by the Commission with a single electronic device, because a single electronic device is easier to bypass than multiple devices. Therefore, we clarify that two or more separate and distinct electronic devices are necessary to implement the Commission's defense in depth requirements.

67. MidAmerican has not provided the Commission with sufficient detail regarding its concern about the Commission granting a reasonable accommodation for those cases where requiring additional physical devices may add complexity and introduce additional risk not necessary to meet the technical objectives of layered security. However, the

[50] Order No. 706 at P 496.

[51] *Id.* P 497 (emphasis added).

Commission believes that our determination in Order No. 706 to address commenters' concerns about the impact on performance and reliability by allowing Regional Entities to grant justified exceptions based on technical feasibility should also satisfy MidAmerican's concern.[52]

68. With respect to MidAmerican's request that the Commission clarify whether the two or more devices may be of the same type or make, we leave this determination to the ERO, taking into account that the revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment.[53]

2. Encryption as Acceptable Two-Factor Authentication

a. Order No. 706

69. Requirement R2 of CIP-005-1 requires a responsible entity to implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter. Requirement R2.4 requires "strong procedural and technical controls" at enabled external access points "to ensure authenticity of the accessing party, where technically feasible."

70. In Order No. 706, the Commission directed 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. The Commission stated that, 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, we stated that the ERO may identify verification technologies or categories of verification technologies in a reference document.

b. Requests for Clarification or Rehearing

71. MidAmerican asks the Commission to clarify that encryption measures would not satisfy Requirement R2.4. According to MidAmerican, as it understands encryption, it is not used as a method of authentication. Encryption protects data from being viewed

---

[52] *See id.* P 498. For example, we stated that 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.

[53] *Id.* P 501.

during storage or transmission and does not involve the authentication of users. While many encryption products and methodologies include features like Public Key Infrastructure-signed certificates, these features are not part of the encryption portion of the product but instead provide for authentication. Therefore, MidAmerican seeks clarification, or a finding on rehearing, that the Commission did not intend to place the burden of determining whether encryption qualifies as an acceptable form of two-factor authentication on the ERO Reliability Standards development process.

c. Commission Determination

72. The Commission clarifies its statement that encryption is one method to accomplish two-factor authentication. First, we note that Order No. 706 left it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. Further, while MidAmerican is correct that some forms of encryption do not involve the authentication of users, others can be used for verification. As noted by MidAmerican, many encryption products include features like Public Key Infrastructure-signed certificates, which provide for authentication. In addition, certain encryption products, such as data link encryptions, better known as Virtual Private Networks, may provide each user a unique identifier, which can then authenticate the user before allowing access to the encrypted information. Encryption products such as these could, if determined by the ERO in the Reliability Standards development process to be reasonable, satisfy Requirement R2.4.

F. CIP-009-1 – Recovery Plans for Critical Cyber Assets

1. Order No. 706

73. The Commission approved Reliability Standard CIP-009-1, which requires the development, updating, and testing of recovery plans, as well as storage and testing of associated backup data and backup media. Among other things, the Commission directed the ERO to modify Requirement R3 of CIP-009-1 to shorten the 90-day timeline for updating recovery plans. In doing so, we stated that we believed 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.[54] However, the Commission found that the Reliability Standards development process may propose a time period other than 30 days, with justification that such alternate time period is equally efficient and effective.

[54] *Id.* P 731.

2. Requests for Rehearing or Clarification

74. MidAmerican asks the Commission to clarify the start-time for the 30 days allowed for updating recovery plan documentation. MidAmerican notes that the Commission similarly directed the ERO to shorten the documentation requirements in Requirement R9 of CIP-007-1 to document changes resulting from modifications to the system or controls. In that instance, the Commission provided that the shortened period "should begin upon final implementation of the modifications."[55] MidAmerican asks whether the shorter period for updating recovery plans begins: (1) on final implementation of modifications to the critical cyber asset (similar to the period in CIP-007-1); or (2) on completion of the lessons-learned analysis performed following a recovery exercise or in response to an actual event.

3. Commission Determination

75. The Commission will clarify that the shortened window for updating recovery plan documentation would be triggered by any of the following circumstances. When a modification to a system or control requires updating the recovery plan, the shortened window should start upon final implementation of modifications to the system or control. If a lessons-learned analysis performed following a recovery exercise or following an actual event requires updating the recovery plan, the shortened window should start upon completion of the lessons-learned analysis.

The Commission orders:

(A) The requests for rehearing of EEI and MidAmerican are hereby denied, as discussed in the body of this order.

(B) The requests for clarification of EEI, MidAmerican and ISO/RTO Council are hereby granted in part, and denied in part, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

[55] *Id.* P 652.