126 FERC ¶ 61,229
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. RM06-22-000; Order No. 706-B]

Mandatory Reliability Standards for Critical Infrastructure Protection

(Issued March 19, 2009)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Order On Clarification.

SUMMARY: The Commission clarifies that the facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706.

EFFECTIVE DATE: This rule will become effective [the date of publication in the **FEDERAL REGISTER**]

FOR FURTHER INFORMATION CONTACT:

Jonathan First (Legal Information)
Office of General Counsel
888 First Street, NE.
Washington, DC 20426
(202) 502-8529

Regis Binder (Technical Information)
Office of Electric Reliability
888 First Street, NE.
Washington, DC 20426
(301) 665-1601

SUPPLEMENTARY INFORMATION:

126 FERC ¶ 61,229
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

Mandatory Reliability Standards for Critical Infrastructure Protection — Docket No. RM06-22-000

ORDER NO. 706-B

ORDER ON CLARIFICATION

(Issued March 19, 2009)

1. In this order, the Commission clarifies the scope of the Critical Infrastructure Protection (CIP) Reliability Standards approved in Order No. 706[1] to assure that no "gap" occurs in the applicability of these Standards.[2] In particular, each of the CIP Reliability Standards provides that facilities regulated by the U.S. Nuclear Regulatory Commission (NRC) are exempt from the Standard. It has come to the attention of the Commission that NRC regulations do not extend to all equipment within a nuclear power plant. Thus, to assure that there is no "gap" in the regulatory process, the Commission clarifies that the "balance of plant" equipment within a nuclear power plant in the United

[1] Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706, 122 FERC ¶ 61,040, order on reh'g, Order No. 706-A, 123 FERC ¶ 61,174 (2008).

[2] CIP Reliability Standards CIP-002-1 through CIP-009-1 (CIP Reliability Standards) were approved by Order No. 706. Reliability Standard CIP-001-1, which pertains to sabotage reporting, was not a subject of Order No. 706 and does not include the exemption statement that is the subject of this order.

States that is not regulated by the NRC is subject to compliance with the CIP Reliability Standards approved in Order No. 706.

I. Background

2. The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), developed the CIP Reliability Standards that require certain users, owners and operators of the Bulk-Power System, including generator owners and operators, to comply with specific requirements to safeguard critical cyber assets. In January 2008, pursuant to section 215 of the Federal Power Act (FPA),[3] the Commission approved the CIP Reliability Standards. In addition, pursuant to section 215(d)(5) of the FPA,[4] the Commission directed the ERO to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission.

3. Each CIP Reliability Standard includes an exemption for facilities regulated by the NRC. For example, Reliability Standard CIP-002-1 provides:

> The following are exempt from Standard CIP-002: Facilities regulated by the U.S. Nuclear Regulatory Commission . . . .[5]

4. In an April 8, 2008 public joint meeting of the Commission and the NRC, staff of both Commissions discussed cyber security at nuclear power plants. While indicating

---

[3] 16 U.S.C. 824o (2006).

[4] 16 U.S.C. 824o(d)(5)(2006).

[5] Reliability Standard CIP-002-1, section 4.2 (Applicability).

that the NRC has proposed regulations to address cyber security at nuclear power plants, NRC staff raised a concern regarding a potential gap in regulatory coverage.[6] In particular, NRC staff indicated that the NRC's proposed regulations on cyber security would not apply to all systems within a nuclear power plant. NRC staff explained:

> The NRC's cyber requirements are not going to extend to power continuity systems. They do not extend directly to what is not directly associated with reactor safety security or emergency response. . . .
>
> As a result, and when you look at the CIP standards that were issued, there is a discrete statement in each of the seven or eight standards where it specifically exempts facilities regulated by the United States Nuclear Regulatory Commission from compliance with those CIP Standards. So there is an issue there in the sense that our regulations for cyber security go up to a certain point, and end.[7]

5. On September 18, 2008, the Commission issued an Order on Proposed Clarification,[8] explaining its concern that a gap may exist in the regulatory process due to the provision in each of the CIP Reliability Standards exempting "facilities regulated by

---

[6] In December 2008, the NRC approved a final rule that included cyber security-related regulations applicable to nuclear power plant licensees. The regulations, referred to herein as the "NRC cyber security regulations," have not been published in the Federal Register at this time and are not currently in effect. They will be codified at 10 CFR 73.54. See Final Rulemaking – Power Reactor Security Requirements, SECY-08-0099 (Jul. 9, 2008); Press Release: NRC Approves Final Rule Expanding Security Requirements for Nuclear Power Plants, (Dec. 17, 2008), available at http://www.nrc.gov/reading-rm/doc-collections/news/2008/08-227.html.

[7] April 8, 2008, Joint Meeting of the Nuclear Regulatory Commission and Federal Energy Regulatory Commission, Tr. at 77-78.

[8] Mandatory Reliability Standards for Critical Infrastructure Protection, Order on Proposed Clarification, 124 FERC ¶ 61,247 (2008) (Proposed Clarification).

the U.S. Nuclear Regulatory Commission." On the understanding that some facilities within a nuclear power plant would not be subject to compliance with cyber security regulations developed by the NRC, the Commission proposed to clarify that the facilities within a nuclear power plant in the United States that are not regulated by the NRC are subject to compliance with the CIP Reliability Standards approved in Order No. 706. The Commission explained its proposal and sought comment on not only the Proposed Clarification, but also two additional questions: (1) whether a clear delineation exists between those facilities in a nuclear power plant which relate to safety and security, and the non-safety related "balance of plant," and if a clear delineation does not exist, whether there is a need for owners and/or operators of nuclear power plants to identify the specific facilities that pertain to reactor safety, security or emergency response and are subject to NRC jurisdiction, and the balance of plant that is subject to the eight CIP Reliability Standards; and (2) if nuclear power plants were to be required to implement the CIP Reliability Standards, whether Table 3 of the implementation plan approved in Order No. 706 should control the implementation schedule.[9]

6. The Proposed Clarification was published in the Federal Register, 73 FR 55,459 (Sept. 25, 2008). In response, comments were filed by 23 interested persons, 17 of which own and/or operate nuclear power plants. A list of the commenters appears in the

[9] Proposed Clarification, 124 FERC ¶ 61,247 at P 9.

Appendix to this Order. These comments have assisted the Commission and are addressed in the discussion, below.

II. Discussion

7. For the reasons discussed below, the Commission finds that the CIP Reliability Standards are applicable to all equipment within a nuclear power plant located in the United States that will not be subject to NRC's cyber security regulations. The thrust of many comments is that the NRC regulates the entire nuclear power plant including power continuity systems and, therefore, the Commission's Proposed Clarification is unnecessary. The Commission is not persuaded by these arguments, which either reference back to voluntary industry standards developed by the nuclear industry, or mischaracterize the nature and extent of NRC's regulations with regard to the entire nuclear power plant. Indeed, NRC Staff comments reiterate that many portions of a nuclear power plant are not regulated by NRC.

8. Nuclear power plants can have a significant effect on the reliability of the Bulk-Power System. Prior to the enactment of section 215 of the FPA, the electric industry had voluntary cyber security provisions and a system of self-certifications. However, Congress imposed a framework for mandatory and enforceable Reliability Standards, explicitly including cyber security, applicable to all users, owners and operators of the Bulk-Power System. That framework charges the Commission with the oversight of the development and enforcement of the Reliability Standards.

9. In previous orders, the Commission has emphasized that the application of the Reliability Standards must remain uniform and consistent.[10] This is necessary both to protect the reliability of the Bulk-Power System and to ensure equity in the application of Reliability Standards. The Commission has found that "section 215 seeks to prevent an instability, an uncontrolled separation or a cascading failure, whether resulting from either a sudden disturbance, including a cybersecurity incident, or an unanticipated failure of the system elements." [11] Therefore, compliance monitoring must occur on an ongoing and proactive basis. Due to the preventive aspect of section 215 and the requirements of the Reliability Standards, compliance monitoring and enforcement of the Reliability Standards are not triggered only by a past event or a cyber security incident. The ERO and Regional Entities have several proactive monitoring processes, including, but not limited to, spot checks and audits, to verify that users, owners and operators are in compliance with the Reliability Standards and to maintain the reliable operation of the Bulk-Power System. This order balances the concerns expressed by commenters with the

[10] See 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., Regulations Preambles 2006-2007 ¶ 31,204, at P 41 and P 290 (2006), order on reh'g, Order No. 672-A, FERC Stats. & Regs., Regulations Preambles 2006-2007 ¶ 31,212 (2006); Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, 72 FR 16416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 at P 298 (2007).

[11] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 24, order on reh'g, Order No. 693-A, 120 FERC ¶ 61,053 (2007); see also 16 U.S.C. 824o(a)(4) (2006)(defining Reliable Operation).

Commission's responsibility for consistency, as well as rigor and uniformity in the compliance monitoring and enforcement of the Reliability Standards.

10. In response to comments, we have refined certain aspects of the Proposed Clarification. However, we continue to believe that a gap in the application of appropriate cyber security standards would exist absent our clarification in this Order.

A. Meaning of the Term "Facility"

11. Before addressing our determination on the Proposed Clarification, we discuss a terminology issue raised by NRC Staff, NEI and other commenters. As mentioned above, the CIP Reliability Standards exempt "facilities regulated by the U.S. Nuclear Regulatory Commission." The Proposed Clarification indicated that a nuclear power plant consists of multiple "facilities" within its boundaries, some but not all of which are regulated by the NRC. For example, we stated that "NRC's regulation of a nuclear power plant is limited to the facilities that are associated with reactor safety or emergency response."[12]

Comments

12. Commenters state that the term "facility," as used in the nuclear industry, refers to the entire nuclear power plant. For example, NRC Staff comments that the term "facility" is defined by the Atomic Energy Act of 1954 as a "production or utilization facility," and the term is commonly synonymous with the entire nuclear power plant,

[12] Proposed Clarification, 124 FERC ¶ 61,247 at P 6.

"that comprises the entire set of buildings, cooling towers, assets, switchyards, systems, and equipment within the owner-controlled area . . . ."[13] The NRC Staff asserts that the use of the term "facilities" in the Proposed Clarification might effectively exempt all portions of nuclear power plants from the CIP Reliability Standards and thus not close the regulatory gap that the Commission intended to address. Rather, the NRC Staff explains that, when referring to discrete elements within a nuclear power plant, the NRC generally uses the term, "structures, systems and components."

13. NEI, supported by a number of commenters, similarly states that the Commission used the term "facilities" in a manner that is not consistent with the use of the term in the nuclear industry. NEI states that the nuclear industry typically uses the term "facility" to mean the entire nuclear power plant, and that the equivalent in nuclear parlance of "facilities," as used by the Commission, are the "structures, systems, components and networks ("SSC") which provide the various functions for plant operation and shut down."[14]

Commission Determination

14. It appears that the use of the term "facility" in the Proposed Clarification differs from the common use of that term in the nuclear regulatory environment. For purposes of this order, we use the term "nuclear power plant" to describe the entire nuclear

[13] NRC Staff Comments at 1.

[14] NEI Comments at 2.

generating plant, including the entire set of buildings, cooling towers, assets, switchyards, systems, and equipment within the owner-controlled area. This term is consistent with NRC Staff's explanation.

15. NRC Staff states that it generally uses the term "structures, systems and components" to refer to discrete elements of the nuclear power plant regulated by the NRC, and suggests that the Commission uses "facilities" in an analogous way. We will use the term "structures, systems and components" to reference any element of equipment, systems or networks of equipment, or portions within a nuclear power plant within an entity's ownership or control. NRC Staff follows its description of what structures comprise a nuclear power plant with the note, "many of which are not directly regulated by the NRC." For purposes of this order, we will use the term "balance of plant" to reference those portions of the nuclear power plant to which NRC Staff refers, as that term is defined by the NRC's regulations.[15]

B. Regulatory Gap - Need for the Clarification

16. In the Proposed Clarification, the Commission explained that:

> The plain meaning of the exemption language in the eight CIP Reliability Standards at issue is that only those facilities within a nuclear generation plant that are regulated by the NRC are exempt from those Standards. The

[15] The NRC's regulations define the Balance of Plant as: "the remaining systems, components, and structures that comprise a complete nuclear power plant and are not included in the nuclear steam supply system." The Nuclear Steam Supply System is defined as consisting of "the reactor core, reactor coolant system, and related auxiliary systems including the emergency core cooling system; decay heat removal system; and chemical volume and control system." 10 CFR 170.3 (2008).

> exemption language in the eight CIP Reliability Standards neither states, nor implies, that all facilities within a nuclear generation plant are exempt from the Standards, regardless of whether they are subject to NRC regulation. However, the Commission believes there is a need to assure that there is no potential gap in the regulation of critical cyber assets at nuclear generation plants.[16]

The Commission, thus, proposed to clarify that Reliability Standards CIP-002-1 through CIP-009-1 apply to the facilities, i.e., structures, systems and components, within a nuclear power plant that are not regulated by the NRC.

Comments

17. NRC Staff and NERC agree with the Commission that clarification of the CIP Reliability Standards is needed. NEI and other stakeholders in the nuclear industry oppose the clarification, arguing that it is unnecessary because no regulatory gap exists since the NRC's jurisdiction can reach all equipment at nuclear power plants that might need cyber security protection.

18. NRC Staff comments that much of the equipment within the owner-controlled area of the nuclear power plant is not directly regulated by the NRC. Thus, NRC Staff supports the Commission's proposal and suggests certain refinements to the proposal to provide additional clarity to distinguish "the scope of plant functions that are subject to

[16] Proposed Clarification, 124 FERC ¶ 61,247 at P 7 (emphasis in original). As discussed above, the term facilities as used in the Proposed Clarification was intended to apply to structures, systems and components within a nuclear power plant.

NRC requirements from those functions that are subject to applicable FERC-regulated grid reliability requirements."[17]

19. NERC states that it agrees with the Commission's understanding of the delineation between those "facilities" within a nuclear power plant whose functions are necessary and sufficient for reactor safety, security or emergency response versus the portion of the rest of the plant whose functions are necessary for Bulk-Power System reliability. NERC agrees with the Commission that there is a need for more clarity with regard to the applicability of CIP Reliability Standards to nuclear power plants, and recommends an expedited modification to the Standards.

20. NEI, and other commenters,[18] many of which support NEI's comments, assert that the Commission's Proposed Clarification is unnecessary, as there is no regulatory gap in the oversight of critical cyber assets at nuclear power plants. According to NEI and others, the NRC regulates the entire nuclear power plant, including cyber security for balance of plant systems that may be critical to Bulk-Power System reliability. Commenters identify three sources of NRC's authority: the nuclear industry's comprehensive security program developed by NEI (NEI 04-04), NRC's "Maintenance Rule," and NRC's recently-promulgated cyber security rules. In addition, NEI and others

[17] NRC Comments at 1.

[18] E.g., AEP, Ameren, Arizona Public Service, Dominion, Duke, Entergy, Exelon, FirstEnergy, Luminant, PG&E, PPL Companies, PSEG, and Wolf Creek.

contend that application of CIP Reliability Standards to nuclear power plants would result in dual regulation of equipment, which would be complicated and inefficient.

Nuclear Industry Cyber Security Guideline, NEI 04-04

21. NEI and other commenters[19] argue that the application of CIP Reliability Standards is not warranted because the nuclear industry has made a binding commitment to implement a comprehensive cyber security program developed by NEI and endorsed by NRC.[20] NEI explains that, pursuant to this program, existing digital assets at nuclear power plants are analyzed for cyber vulnerabilities and necessary mitigation plans are established and implemented. According to NEI, all nuclear power plants implemented NEI 04-04 on or before May 1, 2008.

22. NEI explains that, in February 2002, the NRC issued Order EA-02-026, "Interim Safeguards and Security Compensation Measures for Nuclear Power Plants,"[21] which included required actions to address cyber security concerns. According to NEI, as a "supplement" to implementation of this NRC order, the nuclear industry committed to implement NEI 04-04, which was designed to protect plant systems, including all those pertinent to balance of plant. NEI states that implementation of the NEI 04-04 cyber

[19] E.g., AEP, Arizona Public Service, Duke, Exelon, Luminant, PG&E, PSEG, Southern and Wolf Creek.

[20] NEI Comments at 5-8, citing to NEI 04-04 Revision 1, "Power Security Program for Nuclear Reactors" (April 2006) (NEI 04-04).

[21] All Operating Power Licensees; Order Modifying Licenses, 67 FR 9792 (Mar. 4, 2002).

security program extends to plant generation equipment up to and including the first breaker out from the main transformer to the switchyard breaker. According to NEI, in response to a system vulnerability identified in 2007, both industry and NRC relied on NEI 04-04 in determining that the first breaker out from the transformer to the switchyard is within the boundary of the nuclear power plant.[22]

23. NEI states that, in 2005, NRC staff endorsed NEI 04-04 as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. It cites to the NRC Inspection Manual, which states that a performance deficiency can exist if a licensee fails to meet a self-imposed standard. Thus, NEI contends that, because licensees have self-imposed NEI 04-04 through a binding initiative, NRC has the regulatory authority to inspect and enforce the program's requirements.[23]

24. NEI and other commenters, including Duke, Entergy and Exelon, contend that NRC's current oversight is adequate and the existing cyber security program is "functionally equivalent" to the CIP Reliability Standards.

[22] NEI Comments at 6.

[23] Exelon, Luminant and Progress Energy also claim that NEI 04-04 is mandatory and enforceable by NRC. Likewise, APS contends that compliance with NEI 04-04 is not voluntary because, through NEI membership, all nuclear power plants are contractually bound to follow the program.

NRC's Maintenance Rule

25. NEI, Exelon and Southern argue that NRC regulates the "balance of plant," and focus on NRC's "Maintenance Rule" in particular to support their argument.[24] The Maintenance Rule requires a licensee to implement a monitoring program that includes both safety related and non-safety related structures, systems and components.[25] The Maintenance Rule identifies as within the scope of the monitoring program, structures, systems and components:

> (b)(2)(i) That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures; or
> (b)(2)(ii) Whose failure could prevent safety-related structures, systems, and components from fulfilling their safety-related function; or
> (b)(2)(iii) Whose failure could cause a reactor scram or actuation of a safety-related system.[26]

NEI states that NRC may take enforcement action for violations of the Maintenance Rule, and includes examples of citations for failures of non-safety systems. According to NEI, implementing guidance for the Maintenance Rule, developed by industry and endorsed

---

[24] In addition, numerous commenters state that they support NEI's comments. E.g., EEI, AEP, Arizona Public Service, Dominion, Kansas City and PG&E.

[25] Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, 56 FR 31306 (Jul. 10, 1991) (Maintenance Rule). See also 10 CFR 50.65.

[26] 10 CFR 50.65(b)(2)(i)-(iii). NRC's Glossary defines a "scram" as "[t]he sudden shutting down of a nuclear reactor, usually by rapid insertion of control rods, either automatically or manually by the reactor operator. May also be called a reactor trip." NERC Glossary, available at http://www.nrc.gov/reading-rm/basic-ref/glossary.

by NRC, provides further evidence that structures, systems and components pertaining to the balance of plant must be monitored.[27]

26. NEI thus argues that:

> The NRC regulates any [structure, system or component] in a nuclear power plant that has both a direct or indirect impact on safety, security, or emergency response systems. The NRC's regulations extend to all systems that could cause a reactor scram, diminish the ability to mitigate the consequences of a reactor scram, or cause the actuation of a safety system. These are the same systems that constitute the balance of the plant for Continuity of Operations purposes.[28]

According to NEI, the failure of a structure, system or component as the result of a cyber security breach affects the reliability of equipment operation and is consequently within the scope of the Maintenance Rule. Ameren, which owns and operates a nuclear power plant, comments that it is unable to identify any structures, systems or components that are not currently subject to cyber security regulation by the NRC that could impact electric reliability.

NRC Cyber Security Regulations

27. NEI explains that NRC has proposed regulations that would specifically address cyber security at nuclear power plants.[29] According to NEI, Exelon, Progress Energy and

---

[27] NEI Comments at 4, citing NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," and NRC Regulatory Guide 1.160.

[28] NEI Comments at 5.

[29] See supra n. 6.

Southern, NRC's cyber security regulations would apply to both safety functions and "support systems and equipment which if compromised would adversely impact safety, security or emergency preparedness functions."[30] Further, the NRC regulations would require licensees to identify the cyber security assets they will protect under the program, and the list of identified assets becomes the basis for inspection by NRC Staff. NEI states that most balance of plant systems support both nuclear safety and continuity of operations.

28. NEI contends that there are "few, if any," systems within the boundary of a typical nuclear power plant that support only continuity of operations. Thus, according to NEI, since the failure of such systems could cause a reactor scram or actuation of a safety system, the proposed NRC regulation would apply and there would be no regulatory gap. NEI also claims that, as with all NRC regulation, the requirements of 10 CFR 73.54 would be assessed, inspected and enforced.

Dual Regulation

29. NEI, EEI and other commenters[31] express concern that if the Commission issues its Proposed Clarification, dual regulation will result and cause overlapping requirements, contradictory requirements, duplicate inspections and recordkeeping, and duplicate worker training and qualifications. They assert that confusion and conflicts will result

[30] To be codified at 10 CFR 73.54(a)(1)(iv).

[31] E.g., Ameren, Exelon, Progress Energy, PPL and PSEG.

with respect to applicability of regulations if the Commission's clarification separates digital assets within a nuclear power plant into some that are subject to NRC regulations and others that are subject to CIP Reliability Standards. AEP states that the proposed application of the CIP Reliability Standards could result in increased costs and complexity without a commensurate increase in reliability or protection.

30. NEI, EEI and other commenters[32] argue the most effective way to eliminate any potential gap in regulatory oversight is to maintain a single set of regulations for the entire nuclear power plant under the jurisdiction of the NRC. IESO/Hydro One assert that nuclear power plants should only be regulated by one entity, and cyber security at nuclear power plants must be under the jurisdiction of the NRC or the Canadian nuclear authority.

Commission Determination

31. As discussed below, the Commission is not persuaded by the nuclear industry commenters' arguments that the NRC regulates all balance of plant equipment within a nuclear power plant.

Voluntary Industry Standard NEI 04-04

32. The nuclear industry's development of a cyber security program under NEI 04-04 is commendable. However, compliance with NEI 04-04 is voluntary. As mandated by the Energy Policy Act of 2005, the Commission must ensure that the Commission-

[32] E.g., Arizona Public Service, Entergy, PSEG, Dominion, Exelon, Luminant, Ontario Power, Southern, Wolf Creek, and PG&E.

certified ERO develops Reliability Standards and provides for consistent monitoring and enforcement of such standards. The nuclear industry's voluntary commitment to NEI 04-04 does not satisfy the Energy Policy Act's mandate and is not adequate assurance that the reliability of the Bulk-Power System is protected. Therefore, the Commission cannot rely upon NEI 04-04 to meet its obligations under the Energy Policy Act of 2005.

33. While NEI maintains that NEI 04-04 is subject to NRC regulatory and enforcement authority, NRC Staff has disavowed this position with regard to non-safety security and emergency preparedness related cyber security assets within a nuclear power plant.[33] While NEI characterizes NEI 04-04 as a "supplement" to NRC Order EA-02-026, the NRC order did not mandate the development and implementation of the industry-developed program. We understand that, on occasion, NRC Staff will endorse an industry-developed program or guidance document as one acceptable manner to comply with NRC regulations. The industry-developed cyber security program, however, was not developed as a means to comply with an NRC regulation. Thus, while the NRC Staff simply endorsed NEI 04-04 as "an acceptable method for establishing and maintaining a cyber security program at nuclear power plants,"[34] the scope of this

[33] NRC Staff Comments at 1.

[34] NEI Comments, Appendix E (December 23, 2005 letter from NRC, Director, Office of Nuclear Security and Incident Response to NEI, Vice President, Nuclear Operations).

endorsement falls short of documenting that NEI 04-04 is mandatory and enforceable by the NRC.

34. Further, we do not agree with commenters' claims that NEI 04-04 is mandatory because entities have made a contractually binding commitment to NEI to implement the program. Again, while such proactive commitments by industry are laudable, they do not and cannot substitute for a government regulation subject to compliance and enforcement, including civil penalties for non-compliance.

NRC Regulations

35. The Commission also rejects the claim of NEI and other commenters that there is no regulatory gap and the Commission's clarification is unnecessary because relevant NRC regulations apply to all structures, systems and components within a nuclear power plant, both safety and non-safety related, including the equipment in the balance of plant.

36. Commenters point to NRC's Maintenance Rule, which requires nuclear power plant licensees to monitor the effectiveness of maintenance activities for safety-significant plant equipment. In promulgating the Maintenance Rule, NRC explained that, while it considered having the rule apply to all structures, systems and components in a nuclear power plant, including the balance of plant, the final rule was more limited.[35] While the Maintenance Rule expressly includes both safety related and non-safety related

[35] Maintenance Rule, 56 FR 31306 at 31314-15. NRC indicated that this limitation of the scope was in part a reaction to commenter concerns that "many [structures, systems or components] in the [balance of plant] have no nexus to public health and safety . . . ." Id. at 31315.

(i.e., balance of plant) structures, systems and components, NRC limited the scope of the rule to include only those balance of plant structures, systems and components "whose failure could most directly threaten public health and safety."[36] This limitation is set forth in subsection (b) of the Maintenance Rule, which describes the scope of the maintenance monitoring program required pursuant to subsection (a) of the rule. In sum, the Maintenance Rule contemplates that there will be balance of plant structures, systems and components that are not subject to the rule.

37. NEI and other commenters also claim that the NRC's then-proposed, and now recently approved, cyber security regulations demonstrate that there is, in fact, no regulatory gap. However, as indicated by the NRC Staff's comments, the NRC cyber security regulations have limited application to balance of plant. The NRC cyber security regulations will apply to safety-related functions, security functions, emergency preparedness and "support systems and equipment which, if compromised, would adversely impact safety security and emergency preparedness functions."[37]

---

[36] Id. at 31315. NRC explained that this scope is consistent with NRC's authority pursuant to sections 161 and 182 of the Atomic Energy Act to protect the public health and safety related to nuclear power plant safety. Id. at 31314-15. See also Pacific Gas & Electric Corp. v. State Energy Resources & Conservation and Development Commission, 461 U.S. 190, 210 n.22 (1983) (concluding that the Atomic Energy Act did not displace other agencies' – Federal, state and local – jurisdiction over the generation, sale and transmission of electric energy, as the NRC's jurisdiction was limited to the protection of the public's health and safety from the particular risks posed by nuclear material); English v. General Electric Co., 496 U.S. 76, 82 (1990) (finding "NRC … is concerned primarily with public health and safety").

[37] See supra n. 6, to be codified at 10 CFR 73.54(a)(1)(iv).

38. We disagree with nuclear industry commenters that contend that this latter provision is so broad as to include the entire balance of plant. Rather, similar to the Maintenance Rule, this provision identifies a subset of non-safety structures, systems and components that are subject to the NRC cyber security regulations. The remainder of the balance of plant equipment will not be subject to the NRC cyber security regulations. NRC Staff apprised the Commission of this limitation and the potential for a regulatory gap at a public meeting of the two commissions, when stating "The NRC's cyber requirements are not going to extend to power continuity systems. They do not extend directly to what is not directly associated with reactor safety, security or emergency response."[38]

Dual Regulation

39. Numerous nuclear industry commenters raise concerns that the Commission's proposal would result in nuclear power plant licensees having to comply with two sets of regulations, both NRC regulations and CIP Reliability Standards. According to commenters, this would likely cause overlapping requirements, contradictory requirements, duplicate inspections and other burdens.

[38] Proposed Clarification Order, 124 FERC ¶ 61,247 at P 5, quoting April 8, 2008, Joint Meeting of the NRC and the Commission, Tr. at 77-78. Likewise, in its written comments, NRC staff explains that "[t]he NRC regards 'facility' as referring to the entire power generating plant, that comprises the entire set of buildings, cooling towers, assets, switchyards, systems and equipment within the owner-controlled area, many of which are not directly regulated by the NRC." NRC Staff Comments at 1 (emphasis added).

40. The Commission is not persuaded by these comments. First, the Commission believes that the possible burden, confusion and inefficiency is speculative, and may well be overstated by commenters. We note that no commenter states that any of the CIP Reliability Standards conflict with the NRC's cyber security regulations. While transition issues will invariably occur, it is possible that, for example, nuclear power plant licensees can minimize any possible burden by developing a single operating manual that integrates both NRC regulations and CIP Reliability Standards. In any case, commenters have not set forth an adequate justification for the Commission and the ERO to forego their authority so that certain critical cyber assets are not subject to any mandatory oversight. In addition, we believe that concerns over possible contradictory requirements or duplicative inspections may be addressed through further regulatory coordination, discussed below.

C. Delineation of Equipment Within a Nuclear Power Plant and Modification of the Exemption Text

41. In the Proposed Clarification, the Commission requested comments on whether there is a clear delineation between equipment within a nuclear power plant that pertains to reactor safety, security or emergency response and the non-safety portion of the balance of plant. The Commission asked whether there is a need for owners and/or operators of nuclear power plants to identify the specific facilities that pertain to reactor safety, security or emergency response and subject to NRC regulation, and the balance of plant that is subject to the CIP Reliability Standards.

Comments

42. NEI, Exelon and others[39] assert that there is a clear delineation between equipment within a nuclear power plant related to safety and security and equipment that constitutes balance of plant. NEI comments that under the existing nuclear cyber security programs, all digital assets have been identified and evaluated, and cyber security risk parameters have been established for assets which are nuclear-significant and those needed to maintain continuity of operation. Similarly, Exelon and Southern explain that, due to various designs of nuclear power plants, the delineation may vary from plant to plant. Therefore, each licensee identifies the structures, systems, and components that are "nuclear significant" and those that impact continuity of power, i.e., Bulk-Power System reliability. NEI, Exelon, Southern and other commenters maintain that this delineation is not relevant since NRC cyber security regulations apply to the balance of plant.

43. IESO/Hydro One assert that it is not possible, from either a procedural or technical standpoint, to establish a clear demarcation between facilities that relate to reactor safety or emergency response, and those that relate to reliability of the electric grid since the nuclear plant system is an interconnected and complex model. Breaking up this model would be confusing and technically difficult, according to IESO/Hydro One. Ontario Power notes that there are no "balance of plant" concerns in Canada since the Canadian Nuclear Safety Commission has jurisdiction over the entire nuclear power plant.

[39] E.g., Dominion, Duke, Luminant, PG&E, Southern and Wolf Creek.

44. FirstEnergy asserts that, notwithstanding the ability to delineate between equipment, the Commission's inquiry is premised on the incorrect assumption that a line can be drawn between safety-related facilities regulated by the NRC and non-safety-related facilities that are not directly regulated by the NRC. FirstEnergy comments that, in fact, much equipment within a nuclear power plant that is categorized as balance of plant may have an indirect impact on safety or emergency response. It maintains that any attempt to separate equipment into two groupings for the purpose of creating two cyber security regulatory schemes would be technically challenging, potentially unsafe, and beyond the Commission's general expertise. PSEG and Ameren provide similar comments, and Ameren suggests that the delineation of the specific structures, systems and components regulated by NRC and the Commission should occur on a plant-by-plant basis with an opportunity for the owner or operator to obtain guidance as to whether its categorization is acceptable.

45. On a related matter, several commenters recommend changes to the exemption provision of the CIP Reliability Standards to better delineate the scope of NRC's regulations. NERC states that the delineation provided by its proposed revised exemption language for the Applicability sections of the CIP Reliability Standards is clear and adequately addresses the delineation issues raised by the Commission. For example, NERC proposes to expedite a modification to the exemption provision of the CIP Reliability Standards to reflect that "digital computer and communications systems and networks within a U.S. nuclear power plant . . . that are regulated and enforced by the

U.S. Nuclear Regulatory Commission are exempt from the requirements of this standard."[40] Other commenters also recommend changes to the exemption provision of the CIP Reliability Standards to clarify which equipment would be subject to NRC's cyber security regulations, as opposed to the CIP Reliability Standards. NRC Staff proposes to clarify the exemption as follows: "[a]ll portions of a nuclear power plant . . . that fall within the regulatory jurisdiction and authority pertaining to cyber security of the NRC are exempt from the CIP Reliability Standards . . . ."[41]

46. NEI recommends that the Commission direct NERC to modify the exemption language in the CIP Reliability Standards to state:

> Nuclear safety-related and important-to-safety systems and networks, security systems and networks, emergency preparedness systems and networks including offsite communications, and support systems and equipment which if compromised would adversely impact safety, security or emergency preparedness functions regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.[42]

47. APS, Luminant, PG&E and Wolf Creek offer variations on the NEI proposal. For example, APS supports NEI's suggested change to existing CIP exemption language but would follow the "adversely impact safety," phrase with the additional phrase "plant reliability (continuity of power)."

---

[40] NERC Comments at 3.

[41] NRC Staff Comments at 1.

[42] NEI Comments at 14.

Commission Determination

48. Based on the comments of NEI and other commenters, we understand that nuclear power plant licensees maintain a clear delineation between equipment within a nuclear power plant that pertains to reactor safety, security or emergency response, and equipment that pertains to balance of plant. Further, as discussed above, the NRC's cyber security regulations may apply to certain equipment within the balance of plant in some respects. However, it appears that the delineation of which balance of plant equipment may be subject to the NRC cyber security regulations is not yet fully accomplished and will likely be articulated separately for each nuclear power plant, with the line of regulatory demarcation differing from plant to plant. Moreover, while NRC Staff indicates that there are "many" components of balance of plant that will not be subject to the NRC cyber security regulations, NEI and other industry commenters assert that there are few, if any.

49. To resolve this matter in a manner that assures that no regulatory gap occurs, and also provides certainty to nuclear power plant licensees, the Commission requires that all balance of equipment within a nuclear power plant is subject to the CIP Reliability Standards. This approach provides clarity and certainty because, as indicated above, nuclear power plant licensees understand a clear delineation between equipment within a nuclear power plant that pertains to reactor safety, security or emergency response, and

equipment that pertains to balance of plant. This is certainly with the scope of the Commission's and ERO's authority pursuant to section 215(b) of the FPA.[43]

50. Further, a nuclear power plant licensee may seek an exception from the ERO to the extent that the licensee believes that specific equipment within the balance of plant is subject to NRC cyber security regulations. If the ERO grants the exception, that equipment within the balance of plant would not be subject to compliance with the CIP Reliability Standards. We would expect that the ERO would make such determinations with the consultation of NRC and oversight of Commission staff. Thus, to further the development of this ERO process, the ERO should consider the appropriateness of developing a memorandum of understanding with the NRC, or revising existing agreements, to address such matters as NRC staff consultation in the exception application process and sharing of Safeguard Information. The Commission believes that with the above two-part approach, i.e., subjecting all balance of plant equipment within a nuclear power plant to the CIP Reliability Standards, with exceptions allowed via a process implemented by the ERO, nuclear power plant licensees will have a bright-line rule that eliminates the potential regulatory gap and provides certainty; and a plant-specific equipment exception process to avoid dual regulation where appropriate.

51. While balance of plant equipment will be subject to the CIP Reliability Standards, this does not mean that every such asset must meet all of the requirements of the CIP

[43] 16 U.S.C. 824o(b). Section 215(b) of the FPA sets forth the Commission's jurisdiction over all "users, owners and operators of the bulk-power system."

Reliability Standards. For example, such equipment should be considered pursuant to Reliability Standard CIP-002-1 to identify critical cyber assets.

52. With regard to the recommended changes to the exemption language of the CIP Reliability Standards, we believe that the above discussion adequately addresses our concerns. We leave to the discretion of the ERO whether a modification to further refine the exemption language, to reflect the findings of this order, is needed.

D. Regulatory Coordination

53. NRC Staff recommends the development of a memorandum of understanding to outline scope, clarify agency roles and responsibilities, and provide specific technical requirements related to the application and administration of regulations pertaining to the protection of critical digital assets at nuclear power plants. Similarly, NEI, EEI and other commenters urge a coordinated approach to cyber security oversight at nuclear power plants to avoid redundancies and avoid unnecessary burdens on licensees.

54. Further, EEI, Exelon and the PSEG Companies request that the Commission consider the roles of the ERO and the NRC in the application, enforcement and administration of the CIP Reliability Standards as applied to nuclear power plants, including considering the implications of the Safeguards Information requirements set forth in 10 CFR 73.22.

Commission Determination

55. We agree that it is advisable for the two commissions to coordinate their respective cyber security-related activities with regard to nuclear power plants. However,

for purposes of this proceeding, we need not resolve this question regarding the need for a memorandum of understanding between the two commissions.

E. Implementation Schedule

56. The Proposed Clarification requested comment on an appropriate implementation schedule timetable for owners and operators of nuclear power plants to comply with the CIP Reliability Standards. In Order No. 706, the Commission approved NERC's staggered implementation schedule for the CIP Reliability Standards. Table 3 of NERC's Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 defines the implementation schedule for Responsible Entities that were required to register during 2006. Under Table 3, Responsible Entities must be Auditably Compliant with CIP-002-1 through CIP-009-1 by December 31, 2010.[44]

57. NERC supports the application of Table 3 of the CIP Reliability Standards implementation plan to determine an appropriate compliance schedule.[45] In contrast, numerous nuclear industry commenters[46] argue that the Table 3 implementation schedule should not apply to nuclear power plants. Rather, many of the nuclear industry commenters suggest that the Commission should direct NERC to work with stakeholders

---

[44] Proposed Clarification, 124 FERC ¶ 61,247 at P 9.

[45] Order No. 706, Mandatory Reliability Standards for Critical Infrastructure Protection, 122 FERC ¶ 61,040, at P 77-90 (2008).

[46] E.g., Ameren, Dominion, Duke, EEI, Exelon, FirstEnergy, IESO/Hydro One, Ontario Power, PG&E, PPL, PSEG, Southern and Wolf Creek.

to develop an appropriate timeframe for owners and operators of nuclear power plants to achieve full compliance with the CIP Reliability Standards.

58. NEI recommends a schedule similar to Table 4 of NERC's Implementation Plan for Cyber Security Standards, which pertains to compliance deadlines for newly registered entities. Exelon proposes a "begin work" date of December 31, 2008, with an auditable compliance deadline of December 31, 2011.

Commission Determination

59. The Commission finds that it is not appropriate to dictate the schedule contained in Table 3 of NERC's Implementation Plan, i.e., a December 2010 deadline for auditable compliance, for nuclear power plants to comply with the CIP Reliability Standards. Instead of requiring nuclear power plants to implement the CIP Reliability Standards on a fixed schedule at this time, we agree to allow more flexibility.

60. Rather than the Commission setting an implementation schedule, we agree with commenters that the ERO should develop an appropriate schedule after providing for stakeholder input. Accordingly, we direct the ERO to engage in a stakeholder process to develop a more appropriate timeframe for nuclear power plants' full compliance with CIP Reliability Standards. Further, we direct NERC to submit, within 180 days of the date of issuance of this order, a compliance filing that sets forth a proposed implementation schedule.

The Commission orders:

(A) The CIP Reliability Standards are clarified, as discussed in the body of this order.

(B) The ERO is hereby directed to establish a stakeholder process to determine the appropriate implementation timetable for nuclear power plants, and submit a compliance filing to the Commission within 180 days of the date of issuance of this order, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

APPENDIX
Commenters

AEP	American Electric Power Service Corporation
Arizona Public Service	Arizona Public Service Company
Detroit Edison	Detroit Edison Company
Dominion	Dominion Resources, Inc.
Duke	Duke Energy Corporation
EEI	Edison Electric Institute
Entergy	Entergy Services, Inc.
Exelon	Exelon Corporation
FirstEnergy	FirstEnergy Service Company
IESO/Hydro One	Independent Electricity System Operator of Ontario (IESO) and Hydro One Networks, Inc.
Kansas City	Kansas City Power & Light Company
Luminant	Luminant Generation Company LLC
NERC	North American Electric Reliability Corporation
NEI	Nuclear Energy Institute
Ontario Power	Ontario Power Generation, Inc.
PG&E	Pacific Gas & Electric
PPL Companies	PPL Companies (PPL Electric Utilities Corporation, PPL Susquehanna, LLC, and PPL EnergyPlus, LLC)
Progress Energy	Progress Energy, Inc.
PSEG Companies	PSEG Companies (Public Service Electric and Gas Company, PSEG Energy Resources and Trade LLC, and PSEG Power LLC)
Southern	Southern Nuclear Operating Company
Union Electric/Ameren	Union Electric Company and Ameren Services Company
NRC Staff	U.S. Nuclear Regulatory Commission Staff
Wolf Creek	Wolf Creek Nuclear Operating Corporation