UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE NUCLEAR ENERGY INSTITUTE ON THE ORDER ON PROPOSED CLARIFICATION OF MANDATORY RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION

I. BACKGROUND

On September 25, 2008, the Federal Energy Regulatory Commission ("FERC" or "Commission") issued an Order on Proposed Clarification of Mandatory Reliability Standards for Critical Infrastructure Protection in the above-captioned docket. 73 Fed. Reg. 55459. Comments were due on October 20, 2008. On October 10, 2008, FERC extended the comment period to November 3, 2008.

In this Order, the Commission proposes to clarify the scope of the eight Critical Infrastructure Protection Standards ("CIP") approved in Order No. 706 to assure that these standards are applied to certain nuclear plant equipment and functions which are not regulated by the Nuclear Regulatory Commission ("NRC"). The Commission states that this clarification is being made because the Standards, when issued, exempted "facilities" regulated by the NRC. Subsequent interactions with the NRC, however, led to questions regarding the extent of the NRC's oversight of cyber security for systems not directly related to nuclear safety and subject to the CIP standards. The Commission's stated intent in issuing the Order is to eliminate any such potential "gap" in the regulation of critical assets and critical cyber assets at nuclear plants. 73 Fed. Reg. 55459.

The Nuclear Energy Institute ("NEI") is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

NEI appreciates the opportunity to provide the following comments on the Order.

As discussed in detail, below, there is, in effect, no regulatory "gap" in terms of systems providing Continuity of Operation and oversight by the NRC. Accordingly, there is no need to issue a final order as envisioned in RM06-22-000.

II. COMMENTS

A. Difficulty Created by the Use of the Term "Facilities" In the Nuclear Context

In the Order on Proposed Clarification, the FERC uses the term "facilities" in a manner that is not consistent with the use of the term in the nuclear industry. This has inadvertently clouded the issue at hand. The nuclear industry typically uses the term facility to mean the entire nuclear power plant. The equivalent in nuclear parlance of "facilities," as used by FERC, are structures, systems, components, and networks ("SSC") which provide the various functions for plant operation and shut down.

In addition, the Proposed Order can be read as stating that the CIP Reliability Standards apply to all SSCs within a nuclear generation plant in the United States and are not regulated by the NRC. This is too broad a statement because there are structures, systems, components, and networks within a nuclear generation plant that are not regulated by the NRC and do not support the reliable operation of the Bulk-Power System. The Potable Water System and Sanitary Water Treatment are two such examples. It should be made clear that the eight CIP Reliability Standards apply to structures, systems, components, and networks within a nuclear generation plant in the United States that are not regulated by the NRC and support the reliable operation of the Bulk-Power System.

Of greatest import in this context, we note that few, if any, SSCs within the boundary of the typical nuclear power plant support only a Continuity of Operation function. Most plant systems, including those characterized as Balance of Plant ("BOP"), have a primary function to support Continuity of Operation, however, failure or compromise of these systems could cause a reactor scram (a rapid shutdown of the nuclear reactor), diminish the ability to mitigate the consequences of a reactor scram, or cause the actuation of a safety system.

The industry's Cyber Security Program for Power Reactors focuses on protecting the cyber security of SSCs irrespective of the SSC's intended function. This approach ensures that the SSCs perform their required function regardless of whether the primary function supports nuclear safety or the Continuity of Operation.

The purpose of the Order on Proposed Clarification is to address a concern which was raised by NRC staff that there may be a regulatory gap in cyber security requirements as they apply to power continuity systems. The following discussion demonstrates that NRC regulatory authority extends to plant generation equipment up to and including the first breaker out from the main transformer to the switchyard relay/breaker; that cyber security for those SSCs is provided under an already established cyber security program; and under proposed regulation 10 CFR 73.54; and that the current program is functionally equivalent to the CIPs.

B) Inspection, Enforcement, and Systems Covered by NRC Regulation

1) Inspections and Enforcement

NRC inspections are an important element of NRC's oversight of operators of commercial power reactors. The NRC authority for its inspection and enforcement program is grounded in the Atomic Energy Act and the Energy Reorganization Act of 1974. NRC regulations implementing this statutory authority are embodied largely in 10 CFR Part 2, subpart B, and 10 CFR Part 50. NRC conducts inspections to ensure that licensees meet applicable regulatory requirements. Inspectors follow the comprehensive guidance contained in the NRC Inspection Manual which contains objectives and procedures used for each type of inspection.

The NRC's Reactor Oversight Process ("ROP") integrates inspection, enforcement and assessment of nuclear power plants using a risk-informed, performance-based method to ensure the appropriate level of NRC oversight of licensees. The process is designed to focus on those plant structures, systems, components and activities that are most risk-significant. NRC conducts a minimum baseline inspection of 2000 hours per reactor per year. These inspections are conducted by the resident inspectors (there are at least two full time resident inspectors at each plant site) and specialists from the regional or national headquarters.

In addition to conducting inspections and investigations, NRC may take various forms of enforcement action, up to and including modifying, suspending or revoking licenses. The NRC may also impose civil penalties and, in some cases, criminal penalties (monetary fines or imprisonment). Alleged or suspected criminal violations are referred to the U. S. Department of Justice.

Each licensee's response to new requirements stemming from regulations developed in the NRC's ongoing rulemaking on cyber security (specifically the programs, processes and activities described in the cyber security plan) will be subject to NRC review to assess compliance with the regulation. All subsequent actions taken by the licensee to implement the program, as well as changes or modifications, will be subject to NRC inspection and enforcement.

Notably, NRC conducts special inspections to review the circumstances surrounding plant operating events, such as, perhaps, a plant trip due to loss of off-site power. These inspections focus on, for example, the root cause of the event, if it was preventable, whether plant personnel and systems/components responded properly, and whether conditions were corrected to avoid recurrence. If during an inspection it is determined that NRC regulations were not followed, appropriate enforcement action would be taken.

2) SSCs Covered by NRC Regulation

Regulation 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants" ("Maintenance Rule") provides one example of how the NRC regulates SSCs in the Balance of Plant. The SSCs covered under the requirements of the Maintenance Rule are as follows:

(b) The scope of the monitoring program specified in paragraph (a)(1) of this section shall include safety related and non-safety related structures, systems, and components, as follows:

(1) Safety-related structures, systems and components that are relied upon to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in Sec. 50.34(a)(1), Sec. 50.67(b)(2), or Sec. 100.11 of this chapter, as applicable.

(2) Non-safety related structures, systems, or components:

(b)(2)(i) That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures ("EOPs"); 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.

(c) The requirements of this section shall be implemented by each licensee no later than July 10, 1996.

Enforcement action may be taken for violations of 10 CFR 50.65 for non-safety systems. Appendix B cites examples of inspection reports for violations of the Maintenance Rule for failures of non-safety systems.

Implementing guidance for the Maintenance Rule is contained in NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." The NRC has endorsed this guidance with Regulatory Guide 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants.[1]"

The balance of plant SSCs are monitored at the plant level. Nuclear generating stations monitor plant level performance using criteria such as the following:

- Unplanned automatic or manual reactor scrams - This indicator is used to monitor the success in improving plant safety by reducing the number of unplanned thermal-hydraulic and reactivity transients resulting from reactor scrams. It also provides an indication of how well the plant is operated and maintained.
- Unplanned Capability Loss Factor ("UCLF") - This indicator is used to monitor the effectiveness of maintenance in minimizing outage time and power reductions that result from unplanned equipment failures or other conditions. It is used to identify precursors to conditions which may lead to challenges to safety systems.
- Unplanned Engineered Safety Feature Actuations ("ESF") - This indicator is used to monitor the effectiveness of maintenance in minimizing unplanned challenges to safety

[1] NUMARC 93-01 discusses the performance criteria used by the NRC to monitor a licensee's compliance with 10 CFR 50.65. Specific performance criteria are established for those structures, systems, and components that are either risk significant or standby mode; the balance is monitored against the overall plant level performance criteria.

systems. This indicator may be monitored at the system level rather than at the plant level.

The NRC regulates any SSC 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.

Many of the non-safety SSCs can cause an unplanned scram, capability loss, or ESF actuation. There are non-safety systems that have more comprehensive monitoring requirements under 10 CRF 50.65 than some safety systems. Meeting the Maintenance Rule performance criteria requires licensees to identify the cause, take corrective actions, and monitor the corrective actions for effectiveness. Failure to do so or having ineffective corrective actions will result in an NRC violation. These actions are applicable regardless of the cause.

The failure of intended operation of a SSC as the result of a cyber security breach introduces a failure mode that affects the reliability of equipment operation and is consequently in the scope of the Maintenance Rule.

C) Cyber Security Programs at Nuclear Power Plants

1) The Nuclear Industry Has Implemented A Comprehensive Cyber Security Program Under NEI 04-04

Nuclear licensees have always been required to maintain a high level of plant security. See 10 CFR Part 73. Since the attacks of September 11, 2001, nuclear licensees implemented additional security measures including many specifically required by the Nuclear Regulatory Commission. The NRC issued Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," February 2002, which included required actions to address cyber security concerns. Although the contents of this Order are protected as Safeguards Information[2] and therefore may not be disclosed herein, the NRC has verified each licensee's compliance with the Order, including those portions establishing cyber security requirements. Specifically, the Order mandates that nuclear power plant licensees identify digital systems critical to the operation of the plant and evaluate the potential consequences to the plant should these systems be compromised.

As a supplement to implementation of the Order, the industry committed to implement NEI 04-04 Revision 1. NEI 04-04 was designed to protect plant systems including all those pertinent to Continuity of Operations.

[2] Safeguards Information is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected. Safeguards Information ("SGI") concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material. While SGI is considered to be sensitive unclassified information, its handling and protection more closely resemble the handling of classified Confidential Information than other sensitive unclassified information.

The nuclear industry developed cyber security programs for the following systems:

- Safety related
- Important to safety
- Auxiliary (those that are necessary for safety systems to accomplish their safety functions)
- Site security
- Emergency response (including off site communication systems)
- Balance of Plant/Continuity of Power (systems having a direct impact on the ability to generate electric power that are required, by regulations or other commitments, for plant operation)

The implementation of the NEI 04-04 cyber security program for these systems extends to plant generation equipment up to and including the first breaker out from the main transformer to the switchyard relay/breaker, which are subject to NRC regulatory oversight. This demarcation point was utilized in licensee responses to address control system cyber security vulnerabilities.

For instance, a control system vulnerability documented in "Mitigation Requirements for the Nuclear Sector to Prevent Intrusive Closures into Electrical Rotating Equipment" (original dated June 19, 2007, revision 1 dated July 19, 2007), became known in the industry as "The Aurora Threat." In response the industry completed an initiative to address the threat, implementation of which was monitored by the NRC. The NRC sent a letter on June 22, 2007, to licensees on control system vulnerabilities and asked licensees to inform the agency of onsite conditions, mitigation actions, completion dates and safety, security and regulatory implications of the 60 day actions. The NRC noted that its letter had been coordinated with the Department of Homeland Security ("DHS").

The NRC and DHS relied on NEI 04-04 Revision 1 to determine that the first breaker out from the transformer to the switchyard is within the boundary of the nuclear generation facility. Systems and components "downstream" of the first breaker out from the transformer to the switchyard come under the purview of NERC standards for the Electricity Sector under CIP-002 through CIP-009.

The industry's initial response to Aurora was driven by DHS and focused on protection of the electric grid. Precedent for NRC regulation of Continuity of Operation equipment, such as Digital Protection and Control Devices ("DPCD"), was established as a part of the directive to respond to the Aurora threat. The NRC subsequently required licensees to respond to Requests for Additional Information ("RAI") covering accident mitigation systems. Subsequent RAIs from NRC clarified certain actions taken with respect to the DPCDs subject to the Aurora scenario. Additionally, the RAIs specified that Aurora-related information be retained for subsequent inspection by the NRC.

The response to the Aurora threat reinforced the boundary delineation for NRC oversight as the systems in the nuclear generation plant inside the first breaker out from the transformer to the switchyard.

2) Adoption and Integration of the NEI 04-04 Program

In April 2006, the nuclear industry agreed to a binding initiative to implement of the Standardized Cyber Security Programs for Power Reactors. As a result of the initiative, each licensee was responsible for developing a cyber security program for each power reactor site in accordance with the guidance in NEI 04-04 Revision 1. The program was implemented by all nuclear generating stations on or before May 1, 2008.

As a part of the industry implementation of the NEI 04-04 program, cyber security policies, processes and procedures were integrated into existing plant programs, including:

- Physical security
- Engineering design control and configuration management
- Accredited training
- Corrective action
- Document control and QA records

The integration of cyber security practices into these programs is designed to ensure that existing digital assets at nuclear power plants are fully analyzed for cyber vulnerabilities, and that necessary mitigation plans are established and implemented. Because of its integration with other plant processes and procedures, the program seeks to minimize the likelihood of new vulnerabilities being introduced during plant changes and modifications.

3) Inspection and Enforcement under the NEI 04-04 Program

In 2005, the NRC staff endorsed NEI 04-04 Revision 1 as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. The NRC endorsement letter is attached at Appendix E.

NRC Inspection Manual 0612 “Power Reactor Inspection Reports” states:

> Performance Deficiency: An issue that is the result of a licensee not meeting a requirement or standard where the cause was reasonably within the licensee’s ability to foresee and correct, and that should have been prevented. A performance deficiency can exist if a licensee fails to meet a self-imposed standard or a standard required by regulation.

Since licensees have self-imposed NEI 04-04 through the industry’s binding initiative, the NRC has the regulatory authority to inspect and enforce the program’s requirements. If there is a Performance Deficiency, the NRC will issue Inspection Findings.

In addition to the industry’s compliance with ORDER EA-02-026 and NEI 04-04, the NRC will implement a strict regulatory regime for security which will include SSCs as defined in the pending 10 CFR 73.54 regulation and other existing NRC programs. NRC regulations apply to all SSCs defined in the Licensing and Design Bases for Nuclear Power Generating Stations

included in the site Design Control and Configuration Management programs and/or other NRC mandated programs.

Existing NRC regulations noted in Appendix A, "Other Governing NRC Regulations," address the nuclear power plant systems, components and networks within the plants, including those systems, components, and networks which also support the reliable operation of the Bulk-Power System. The current division of authority between NRC cyber security requirements and FERC / North American Electric Reliability Corporation ("NERC") cyber security requirements is at the first breaker out from the transformer to the switchyard as previously described.

4) The NEI 04-04 Program Meets the Objectives of the Reliability Standards

To address the adequacy of the level of protection provided to SSCs, NEI has developed a table to cross reference the NERC CIP standards to the provisions which must be met pursuant to NEI 04-04. The tabulation contains information that is security sensitive, and therefore will be provided under separate cover (non-electronic means). The table demonstrates the equivalence between NEI 04-04 and the NERC CIP standards.

5) Proposed Regulation 10 CFR 73.54 for Cyber Security

The NRC has proposed modifications to the 10 CFR Part 73, "Physical Protection of Plants and Materials," The rule is expected to be effective in early 2009. The proposed 10 CFR 73.54 provides a concrete regulatory basis for the creation of a comprehensive cyber security program for all nuclear power reactors.

6) Systems Covered by Proposed Regulation 10 CFR 73.54

Licensees will be required to submit a cyber security plan to the Nuclear Regulatory Commission for review and approval. The site-specific plan must include an implementation schedule.

10 CFR 73.54(a) provides:

> (a) Each licensee shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 73.1
>
> (1) The licensee shall protect digital computer and communication systems and networks associated with
>
> (a)(1)(i) Safety and important to safety functions
>
> (a)(1)(ii) Security systems
>
> (a)(1)(iii) Emergency preparedness functions, including offsite communications;
>
> (a)(1)(iv) Support systems and equipment which if compromised would adversely impact safety, security or emergency preparedness functions.

Further, under 10 CFR 73.54(a)(1), licensees are required to identify the cyber security assets that will be protected under the cyber security program. The rule requires that each licensee will

analyze the digital computer and communication systems and networks in use at their facility to identify those assets that require protection and that the licensee's cyber security program will include measures for the protection of the digital computer and communication systems and networks identified by the licensee through the required analysis. This list of assets becomes the basis for inspection by NRC staff.

The Maintenance Rule and proposed regulation 10 CFR 73.54 provide a means for identifying the Balance of Plant SSCs that would have a secondary function of supporting the Continuity of Operation and be regulated by the NRC.

In order to identify the SSCs that would be protected under the program created as outlined in proposed regulation 10 CFR 73.54, a representative list of systems used at both pressurized water reactors ("PWRs") and boiling water reactors ("BWRs") throughout the U.S. nuclear industry was developed. Appendix D to this document, "Proposed 10 CFR 73.54 Regulatory Decision Tree," provides the decision criteria used to map those SSCs to criteria of 10 CFR 73.54 to identify the systems protected under the cyber security regulation. Appendix C, "Criteria for Categorizing Nuclear Plant Equipment," defines the decision criteria reflected in the Appendix D decision tree by taking into consideration causes, conditions or other existing NRC regulation.

There are few, if any, systems within the boundary of the typical nuclear power plant that support only Continuity of Operations. Most systems, including those characterized as "Balance of Plant," support a dual purpose, both nuclear safety, and Continuity of Operations. However, since the failure or compromise of such systems could cause a reactor scram or actuation of a safety system, they are covered by NRC regulation. Depending on plant configuration, very few systems, or none at all fall, outside of the NRC regulatory scope but play a role in the reliability of the Bulk-Power System is.

NERC staff expressed concern over the term "high assurance" used in 10 CFR 73.54(a). In the context of NRC regulation, high assurance is demonstrated by integration of cyber security defensive strategy elements into existing NRC mandated programs such as Configuration Management, Engineering Design Control, Accredited Training, Corrective Action, Document Control and QA Records. Compliance is monitored through methods such as periodic assessment, independent oversight, and NRC inspection.

In FERC Order RM-06-22-000, the NRC is quoted as stating "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…" The industry acknowledges the agency's stated view that it does not have authority to regulate the power continuity systems, however at a plant system level, digital control systems are already governed by various NRC regulations including 10 CFR 50.65 and proposed rule 10 CFR 73.54. The net effect is that these systems are currently regulated for cyber security failure modes.

7) Inspection and Enforcement Under Proposed Regulation 10 CFR 73.54

As with all NRC regulation, the requirements of 10 CFR 73.54 will be assessed, inspected, and enforced. The proposed regulation 10 CFR 73.54 will require licensees to develop and maintain

written policies and implementing procedures to establish the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee are subject to inspection by NRC staff on a periodic basis. All records and supporting technical documentation must be maintained for a minimum of 3 years.

The proposed modification to 10 CFR 73.55(m) requires the cyber security program to be reviewed at least every 24 months. The review must determine the effectiveness of the cyber security programs, safety/security interface, activities, testing, maintenance, and calibration programs. The results must be documented in a report to the licensee's plant manager and to corporate management. These reports must be maintained in an auditable form and available for inspection by the NRC. Findings from onsite physical protection program reviews must be entered into the site corrective action program.

8) Ongoing Relationship Between the Nuclear Industry and NERC

In February, 2006, the Nuclear Energy Institute, on behalf of the industry, entered into a Memorandum of Agreement with the NERC[3] to establish a continuing, cooperative relationship, facilitate consultation regarding technical information potentially useful in the areas of mutual interest, and promote and encourage free flow of such information.

The MOA describes how NERC and NEI will coordinate on cyber security issues. The MOA provides for the following:

A. NEI will provide guidelines for Nuclear Power Generation Facilities that achieve a level of protection for grid reliability equivalent to that provided in the current and future NERC standards.

B. NERC acknowledges that NEI will provide to NERC cyber security guidelines, NEI 04-04, and any subsequently developed guidelines related to maintaining Continuity of Operation at nuclear power generation facilities.

C. NERC and NEI will share any information learned through reports from licensees or other sources of cyber events that could affect cyber protection of generation assets.

D. Shared information will, where required, be protected from public disclosure as discussed in the MOA.

Given this agreement, NEI believes that areas of concern that may arise in the future with respect to interaction between nuclear generators and the reliability of the Bulk-Power System can be handled through the very consultation and cooperation contemplated by the MOA.

[3] The MOA applies to information related to physical security, cyber security, and Bulk-Power System reliability at U.S. nuclear power plant sites and within the Bulk-Power System that is developed by NERC, NEI, or NEI members, and that is in the parties' possession and/or under their control.

D. The NRC's Regulatory Oversight Is Adequate to Ensure Nuclear Plants Meet the Objectives of the CIP Reliability Standards

The nuclear industry is concerned that certain language in the proposed Order may subject certain SSCs in the nuclear generating plants to regulation, inspection, and reporting requirements by both the FERC and NRC. Dual regulation may result in two sets of regulatory requirements some of which may be in conflict, cause duplicate inspections of the same systems, and impose two sets of qualifications for plant workers. More complex regulation could create error precursor conditions and/or increase cyber security risk to nuclear plant digital assets.

NEI fully supports and concurs with the Commission statement that: "The Commission reaffirms the language of the CIP Reliability Standards - and respects the jurisdiction of the NRC – and does not intend that those Standards apply to facilities within a nuclear generation plant that are regulated by the NRC. This should allay concerns that a specific facility is subject to "dual" regulation by both the Commission and NRC as to cyber security."

To accomplish this, it is most important to establish a clear demarcation point. By practice, the NRC and industry have already established a point of demarcation as the first breaker beyond the main transformer. The NRC's asserted jurisdiction of SSCs whose primary purpose may be Continuity of Operations because they have a secondary effect of challenging safety systems evidences the requisite regulatory oversight. This is codified in the Maintenance Rule. Establishing cyber security as a separate consideration for Bulk-Power Reliability purposes on SSCs that are already regulated by the NRC for Safety and Reliability would, in fact, result in dual regulation.

While NEI's suggested modification to the language of the proposed Order provides necessary clarification to prevent dual regulation, an additional agreement between the FERC and NRC may provide further clarification for interagency purposes. The industry's suggestion is that the FERC and NRC establish one regulatory approach administered by the NRC. This approach should use only one set of standards (e.g., NEI 04-04 or 10 CFR 73.54) and may be memorialized in a Memorandum of Agreement ("MOA") between FERC and NRC. This approach will ensure regulatory stability.

E. Additional Considerations for the Inspection of Cyber Security Programs at Nuclear Power Plants

Two issues that must also be considered are compliance with NRC regulations for the protection of Safeguards Information ("SGI"), and with respect to personnel access authorization programs. Compliance with these requirements will greatly increase the administrative burden on the FERC and NERC.

If FERC asserts regulatory authority over SSCs that are also mentioned in the site security plan, FERC and NERC will have to comply with SGI requirements contained in 10 CFR 73.21, "Requirements for the Protection of Safeguards Information." Inspectors would be subject to access provisions for access to SGI, which is granted based on the results of criminal investigation and other criteria contained in 10 CFR 73.57, "Requirements for Criminal History

Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees," compliance measurements and metrics associated with these SGI systems will also require special protection and access control.

Additionally, the personnel who inspect nuclear generation plants and are granted unescorted access would be required to meet the NRC's access authorization requirements. The unescorted access authorization program includes the following:

- A background investigation designed to identify past actions which are indicative of an individual's future reliability within a protected or vital area of a nuclear power reactor.
- A psychological assessment designed to evaluate the possible impact of any noted psychological characteristics which may have a bearing on trustworthiness and reliability.
- Behavioral observation, conducted by supervisors and management personnel, designed to detect individual behavioral changes which, if left unattended, could lead to acts detrimental to the public health and safety
- Random drug testing.

This would add a significant burden to the FERC and NERC operation as well as to the nuclear NRC licensee who must comply with access authorization requirements.

F. Answers to Specific Questions Posed by FERC Order RM06-22-000

The FERC's Proposed Order RM06-22-000, at paragraph 9, includes two questions.

Question: "Whether there is a clear delineation between those facilities within a nuclear generation plant that pertain to reactor safety security or emergency response and the non-safety portion or, as NRC refers to it, the "balance of plant." For example, the generator itself in a nuclear generation plant would seem to be under the CIP Reliability Standards, but the motors that operate nuclear reactor control rods would seem to be under NRC regulation. If the delineation is not clear, is there a need for owners and/or operators of nuclear generation 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 eight CIP Reliability Standards?"

Response: NEI believes there is a clear delineation between those systems, structures, components, and networks within a nuclear generation plant that are regulated by the NRC. Under the existing nuclear cyber security programs all digital assets were identified, evaluated, and cyber security risk parameters established for both nuclear significant and those digital assets needed to maintain Continuity of Operation. We believe that the NRC regulations for cyber security apply to SSCs within the nuclear generation plant up to and including the first breaker out from the main transformer to the switchyard relay/breaker.

The FERC Order gives the example of the generator as an SSC that would fall under the CIP standards, but the failure of the Generator could cause a reactor trip and plant transient, and thus is currently covered by existing NRC regulation (for example, the Maintenance Rule, 10 CFR

50.65(b)(2)(iii)) and would be covered under proposed cyber security regulation 10 CFR 73.54(a)(1)(iv).

Question: "The Commission seeks comment whether Table 3 for generation owners and generation operators should control the implementation schedule of the CIP Reliability Standards to the facilities within a nuclear generation plant that the NRC does not regulate."

Response: The nuclear industry supports the timely implementation of cyber security measures, but requests the same time as other generators have had to formulate plans that are consistent with Table 3. As previously established, the NRC has jurisdiction of BOP systems. Consequently, we do not believe that FERC should assert jurisdiction and require compliance with the CIP Standards. However, should the Commission decide that certain systems at nuclear facilities must comply with the CIP standards in order to avoid a regulatory "gap," we would respectfully suggest an alternate approach to following the implementation schedule set forth in Table 3. As described in these comments, nuclear generating plants have implemented cyber security measures, but because the current CIP exemption language gives the impression that nuclear power plants would be exempt from compliance with the CIP standards, plants were under the impression that they would be complying with NRC requirements rather than NERC requirements, they may not have planned, staffed, or budgeted for compliance with individual requirements of the CIP standards. Instead, we believe that should the Commission pursue its proposed approach, a schedule similar to that laid out in Table 4 for newly registered entities would be the more appropriate schedule.

III. RECOMMENDATIONS

For the reasons stated above, NEI urges the Commission not to issue a final order clarifying the CIP Reliability Standards as proposed in its September 18, 2008 Order. NEI submits that there is no gap in NRC regulation of cyber security protections for nuclear power plants, and that the Commission's imposition of the NERC standards to the nuclear power systems identified in the Commission's order would create the ambiguity the Commission seeks to dispel. Moreover, imposing NERC standards in addition to the requirements under NRC regulation would create a dual system of regulation that would be unnecessarily costly, that could be in conflict, and that without doubt would be less efficient.

If the Commission rejects these arguments and issues the final order, we respectfully request the following actions be taken in order to affect a meaningful remedy.

Recommended change to the language in the FERC Order to eliminate a perceived Regulatory Gap

> In this order, the Commission proposes to change the scope of the eight Critical Infrastructure Protection (CIP) Reliability Standards approved in Order No. 706 to assure that no regulatory "gap" occurs in the applicability of these Standards. In particular, each of the eight CIP Reliability Standards now provides that structures, systems, components, and networks regulated by the U.S. Nuclear Regulatory Commission (NRC) are exempt from the Standard. It has come to the attention of the Commission that the NRC may not

> regulate all structures, systems, components, and networks within a nuclear generation plant. Thus, to assure that there is no "gap" in the regulatory process, the Commission proposes to change the CIP Reliability Standards to state that the structures, systems, components, and networks within a nuclear generation plant in the United States that are not regulated by the NRC and which support the reliability of the Bulk-Power System are subject to compliance with the eight CIP Reliability Standards approved in Order No. 706.

The revised language, when considering the discussion in these comments would effectively eliminate any perceived "gap" in regulation, would clarify the use of the term "facility," and confirms that the NRC has primary jurisdiction over SSCs at reactor sites.

Establishment of a Memorandum of Agreement between the FERC and NRC

While NEI's suggested modification to the language of the proposed Order provides appropriate clarification to prevent dual regulation from the perspective of the industry, an additional agreement between the FERC and NRC may provide further clarification for interagency purposes. The industry's suggestion is that the FERC and NRC establish one regulatory approach administered by the NRC. This approach should use only one set of standards (e.g., NEI 04-04 or 10 CFR 73.54) and be administratively executed between the FERC and NRC by an instrument such as a Memorandum of Agreement ("MOA") for cyber security. This consolidated approach will ensure regulatory stability.

Recommended Change to the CIP Exemption Language

The nuclear industry recommends that the FERC direct the ERO to modify to the exemption language in the NERC CIP Standards. The current CIP exemption is:

> 4.2. The following are exempt from Standard CIP-002 through CIP-009:
>
> 4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

The nuclear industry recommends that the exemption be maintained, and stated as follows:

> 4.2. The following are exempt from Standard CIP-002 through CIP-009:
>
> 4.2.1 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.

Respectfully submitted,

/s/_____
Alexander Marion
Executive Director, Operations and Engineering
Nuclear Energy Institute
1776 I Street, NW Suite 400
Washington, DC 20006
(202) 739-8080

November 3, 2008

Appendix A

Other Governing NRC Regulations

10 CFR 73.54 Criteria can be mapped to existing NRC regulation. The list of nuclear plant systems subject to this regulation is contained in Appendix C.

(a)(1)(i) Safety and important to safety functions

- 10 CFR 50 Appendix A, General Design Criteria for Nuclear Power Plants
- 10 CFR 50 Appendix B, Quality Assurance criteria for Nuclear Power plants and fuel Reprocessing Plants
- 10 CFR 50 49 Environmental Qualification of Electrical Equipment Important to Safety for Nuclear Power Plants
- 10 CFR 50.62 Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants.
- 10 CFR 50.65, Requirements for Monitoring the Effectiveness of maintenance at Nuclear Power Plants
- 10 CFR 50.59, Changes, Tests, and Experiments
- 10 CFR 54.4, Requirements for the Renewal of Operating Licenses for Nuclear Power Plants - Scope

(a)(1)(ii) Security systems

- 10 CFR 73.55, Requirements for Physical protection of Licensed Activities in nuclear power Reactors Against Radiological Sabotage
- 10 CFR 73.56, Personnel Access Authorization Requirements for Nuclear Power Plants
- 10 CFR 50.59, Changes, Tests, and Experiments
- 10 CFR 54.4, Requirements for the Renewal of Operating Licenses for Nuclear Power Plants - Scope

(a)(1)(iii) Emergency preparedness functions, including offsite communications;

- 10 CRF 50.47, Emergency Plans
- 10 CFR 50.54(q), Conditions of Licenses
- 10 CFR 50.54(t), Conditions of Licenses
- 10 CFR 50 Appendix E, Emergency Planning and Preparedness for Production and Utilization Facilities
- 10 CFR 50.59, Changes, Tests, and Experiments
- 10 CFR 54.4, Requirements for the Renewal of Operating Licenses for Nuclear Power Plants - Scope

(a)(1)(iv) Support systems and equipment which if compromised would adversely impact safety, security or emergency preparedness functions

- 10 CFR 50 Appendix A, General Design Criteria for Nuclear Power Plants (GDC 17, Electric Power System)
- 10 CFR 50.65, Requirements for Monitoring the Effectiveness of maintenance at Nuclear Power Plants
- 10 CFR 50.59, Changes, Tests, and Experiments
- 10 CFR 54.4, Requirements for the Renewal of Operating Licenses for Nuclear Power Plants – Scope
- 10 CFR 50.40 Fire Protection
- 10 CFR 50.61 Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events
- 10 CFR 50.63 Loss of All Alternating Current Power
- 10 CFR 54.21, Contents of Application – Technical Information

Appendix B

Notice of Violation Examples

Inspection Number: 05000369/2008003, Report Date: 07/24/2008

The inspectors identified a green NCV of 10 CFR 50.65(b)(2)(i) for failure to scope the main feedwater tempering line valves into the maintenance rule monitoring program. On May 15, 2008, while reviewing Emergency Operating Procedure feedwater mitigation paths for another issue, the inspectors identified several Unit 1 and Unit 2 main feedwater tempering line valves that are credited in the "response not obtained" column of Emergency Operating Procedure EP/1&2/A/5000/FR-H.1 "Response to Loss of Secondary Heat Sink," for which no preventive maintenance was performed since 1997. Each unit has four separate tempering feedwater flow paths (one to each steam generator) which are used after all other normal and auxiliary feedwater means fail to provide feedwater to the steam generators. None of these flow paths have had flow through them since 1997.

10 CFR 50.65(b)(2)(i) states that non-safety related SSCs used in plant emergency operating procedures shall be scoped in the monitoring program as specified in 10 CFR 50.65(a)(1). Contrary to the above, from May 1997 through May 2008, the licensee failed to adequately scope into the Maintenance Rule several main feedwater tempering line valves used to help mitigate the consequences of an accident in emergency operating procedures.

Inspection Number: 05000327/2008003, Report Date: 08/06/2008

The inspectors identified a Green, non-cited violation (NCV) of 10 CFR 50.65 for failure to include the gland seal steam supply and supply bypass valves in the scope of the maintenance rule program. Isolation of this header was specifically called out in the emergency operating procedures to mitigate a steam generator tube rupture.

On March 8, 2008, during steady state operation, the gland seal regulator on the Unit 2 main turbine failed, resulting in a high steam pressure in the header. This caused the downstream relief valve to lift and increased steam flow, resulting in a small increase in reactor power. When operators attempted to isolate the gland seal header using the motor operated shutoff valve, 2-FCV-47-180, the valve failed to close. The operators subsequently isolated the header using the downstream manual shutoff valve. Because the shutoff valve failed to close, the inspectors reviewed the preventive maintenance performed on the valve and its applicability to the maintenance rule. During this review, the inspectors noted that gland seal steam supply valves 1/2-FCV-47-180 and supply bypass valves 1/2-FCV-47-181 were specifically identified in emergency operating procedure (EOP) E-3, Steam Generator Tube Rupture, Revision 17, as part of the isolation of the main steam header if the Main Steam Isolation Valve (MSIV) failed to close following a steam generator tube rupture. The inspectors reviewed the maintenance rule (10 CFR 50.65) and noted that Paragraph (b)(2)(i) called for non-safety related SSCs used in the plant EOPs to be included in the scope of the rule. In addition, Regulatory Guide (RG) 1.160, Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Revision 2, which provided a means of implementing the maintenance rule, considered SSCs explicitly used in the EOPs as part of the scope of the maintenance rule.

Appendix C

Criteria for Categorizing Nuclear Plant Equipment

The following approach was used to determine the systems, components and networks that are regulated by the NRC.

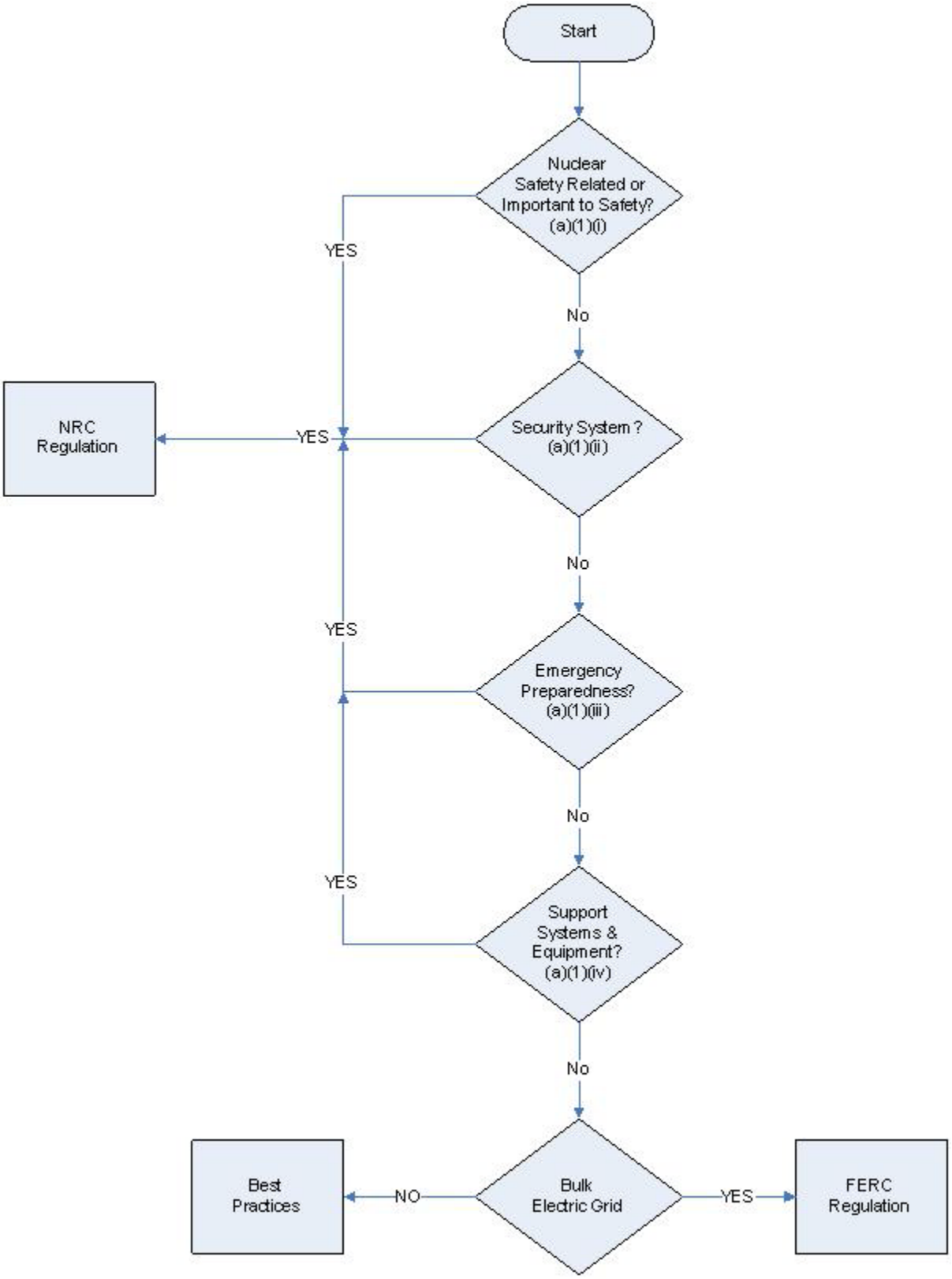
1. *All systems that are Safety Related:* Those structures, systems and components that are relied upon to remain functional during and following design basis events to assure: (1) The integrity of the reactor coolant pressure boundary; (2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in 10 CFR 50.34(a)(1) or 10 CFR 100.11. [e.g., A system credited in the accident analysis of the site Final Safety Analysis Report or Updated Final Safety Analysis Report to meet design basis accident criteria and provide reasonable assurance of protection of public health and safety.]
2. *All systems that are Important to Safety:* All other systems that are important to safety: Non-safety related structures, systems, or components:
   (i) That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs); or
   (ii) Whose failure could prevent safety-related structures, systems, and components from fulfilling their safety-related function; or
   (iii) Whose failure could cause a reactor scram or actuation of a safety-related system.
3. *All Security systems:* Systems that are required by Security to meet the requirements of the Physical Security Plan.
4. *All Emergency Preparedness systems:* Those systems and components required by regulation to notify or provide information to law enforcement, regulators, and federal, state and local agencies should the health and safety of the public be threatened as a result of a nuclear incident.
5. *Support Systems:* Those systems and equipment which, if compromised, would adversely impact safety, security or emergency preparedness functions.

This is summarized by the table below:

Safety Related	**Important to Safety**	**Security**	**Emergency Response**
Probabilistic Risk Assessment Maintenance Rule 10 CFR 50 Accident Mitigation INPO AP 913 (system classification)	Probabilistic Risk Assessment Maintenance Rule 10 CFR 50 Accident Mitigation INPO AP 913 (system classification) Loss of Offsite Power Reactivity Management Reactor Power Reactor Transient Reactor Trip Technical Specifications Selected Licensee Commitments (FSAR) NUREG 0800, Table 7.7-1	10 CFR 73.54 10 CFR 73.55 Security Plan	Emergency Operations Procedures 10 CFR 50 Appendix E Accident Mitigation

Appendix D

Proposed 10 CFR 73.54 Regulatory Decision Tree



Appendix E
NRC Endorsement Letter of NEI 04-04

Endorsement letter is inserted immediately after this page.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 23, 2005

Mr. Michael T. Coyle
Vice President, Nuclear Operations
Nuclear Generation Division
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708

SUBJECT: NRC ACCEPTANCE OF NEI 04-04, "CYBER SECURITY PROGRAM FOR POWER REACTORS," REVISION 1

Dear Mr. Coyle:

The purpose of this letter is to inform you that the U.S. Nuclear Regulatory Commission (NRC) staff finds that Nuclear Energy Institute (NEI) 04-04, "Cyber Security Program for Power Reactors," Revision 1, dated November 18, 2005, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. Additionally, the NRC staff finds that the recommendations provided in the Appendices to NEI 04-04, Revision 1, are an acceptable way to implement the program described in the body of the document.

On June 6, 2005, you submitted NEI 04-04, Revision 0, dated February 28, 2005, on behalf of the industry for NRC staff endorsement. Since that time, the NRC staff has worked closely with the Nuclear Security Working Group's Cyber Security Task Force (the TASK Force) to resolve a number of technical and programmatic concerns and comments. The staff based its concerns and comments on NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," NUREG/CR-6852, "An Examination of Cyber Security at Several U.S. Nuclear Power Plants," International Standard ISO/IEC 17799, "Information Technology - Code of Practice for Information Security Management (ISO/IEC 17799)," and current cyber security practices described in various National Institute of Standards and Technology special publications, and System/Admin Audit Network Security Institute's technical papers.

Subsequently, in a letter dated November 18, 2005, Mr. Jim W. Davis, Director of Operations for the Nuclear Generation Division, NEI, on behalf of the Task Force submitted NEI 04-04, Revision 1, to replace NEI 04-04, Revision 0. The staff reviewed NEI 04-04, Revision 1, and determined that all of the staff's concerns and comments have been adequately addressed.

If you have any questions regarding this matter, please contact Mr. Scott Morris of my staff at (301) 415-7083.

Sincerely,

Roy P. Zimmerman

Roy P. Zimmerman, Director
Office Of Nuclear Security and Incident Response

Document Content(s)