CYBER SECURITY ASSOCIATED WITH
DIGITAL INSTRUMENTATION AND CONTROLS
Interim Staff Guidance-XX

Interim Resolution Regarding Programmatic Implementation of Cyber Security Requirements at Nuclear Power Plants

Issue:

The nuclear power industry requested clarification of differences in guidance associated with implementation of cyber security programs at nuclear power plants. Specifically, the industry asserted that Regulatory Positions 2.1-2.9 provided within Regulatory Guide 1.152 Revision 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants* conflicts with the industry-developed, NRC-accepted NEI 04-04 *Cyber Security Program for Power Reactors, Revision 1,* document with regard to the protection of safety-related digital instrumentation and control systems.

This issue is addressed in the Interim Staff Guidance (ISG) provided below.

Purpose:

The purpose of this ISG is to clarify the NRC staff's guidance with regard to the implementation of cyber security requirements for nuclear power plant safety systems.

Background:

In response to the September 11, 2001 terrorist attacks and subsequent information provided by intelligence and law enforcement agencies, the NRC completed the following actions to enhance the protection of nuclear facilities from both physical and cyber threats:

- NRC Order EA-02-026*, Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants,* February 2002

  This order specified numerous interim compensatory measures to address the elevated threat environment. Part of this order contained cyber security requirements mandating nuclear power plant licensees to identify digital systems critical to the safe operation of the facility, and to evaluate the potential consequences to the facility should these systems be compromised. The material aspects of EA-02-026 are withheld from public disclosure in accordance with 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

- NRC Order EA-03-086*, Design Basis Threat for Radiological Sabotage,* April 2003

  This order supplemented the Design Basis Threat (DBT) for nuclear power plants specified in 10 CFR 73.1. Among other things, this order established requirements for the development of a cyber security program at each nuclear power plant. The material aspects of EA-03-086 are withheld from public disclosure in accordance with 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

DRAFT

- NUREG/CR-6847*, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants,* October 2004

  In conjunction with Pacific Northwest National Laboratory personnel, the NRC staff developed a cyber security self-assessment methodology that could be used by licensees to assess the risk to systems deemed critical to the operation of nuclear power plants. The method was developed utilizing a multidisciplinary team that included nuclear power industry personnel. The material aspects of NUREG/CR-6847 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*."

- NEI 04-04 Revision 1*, Cyber Security Program for Power Reactors,* November 2005

  In a letter dated December 23, 2005, after providing review and comment, the NRC staff notified the Nuclear Energy Institute (NEI) that the industry-generated document, NEI 04-04, Rev. 1, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. The material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*."

- Regulatory Guide 1.152 Revision 2*, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* January 2006

  This document provides specific cyber security guidance for nuclear power plant licensees in the development and implementation of protection measures for digital instrumentation and controls used in safety system applications. This guidance addressed aspects of the implementation of cyber security within safety systems that were not adequately covered in IEEE Standard 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.*

- 71 Federal Register 62664*, Power Reactor Security Requirements - Proposed Rule,* October 26, 2006

  The NRC proposed new cyber security requirements for nuclear power plants in a proposed regulation 10 CFR 73.55 (m). The proposed rule maintains the intent of the previously-issued security orders (i.e., EA-02-026 and EA-03-086) and would require licensees to implement an effective program to detect and prevent cyber attacks on plant computer systems associated with safety, security, and/or emergency response.

- Branch Technical Position 7-14 Revision 5, *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,* March 2007

  This document provides NRC staff review guidelines for evaluating software life-cycle processes associated with safety-related digital instrumentation and control systems at nuclear power plants. It also addresses characteristics that should be present within an acceptable software management plan (e.g., licensees should provide a description of the methods employed to prevent corruption of the software by viruses, Trojan horses or other malicious intrusions).

DRAFT

- 72 Federal Register 12705*, Design Basis Threat – Final Rule,* March 19, 2007

  This final rule requires licensees to protect against "cyber attacks."

- NEI 04-04 Revision 2*, Cyber Security Program for Power Reactors,* August 2007

  Following numerous discussions with NRC staff, industry personnel revised NEI 04-04 primarily to provide clarification with respect to cyber security guidance for safety-related digital instrumentation and control systems. The material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*."

Discussion:

Subsequent to the issuance of NEI 04-04 Rev. 1, as nuclear power plant licensees worked to identify and implement security enhancements to further secure their facilities from internal and external cyber threats, the industry identified differences between certain guidance provided in Regulatory Guide 1.152 and in NEI 04-04, Rev 1. The details of these differences are not described here since NEI 04-04 Rev. 1 is designated as 10 CFR 2.390 information that is exempt from public release under the Freedom of Information Act (5 U.S.C. 522).

In October 2006, the NRC staff, NEI and industry representatives met to discuss methods to resolve the differences between the various guidance documents listed above. Subsequently, an NRC Task Working Group (TWG) was established to address these issues, and to ensure that the cyber security guidance provided was coherent and consistent for both existing licensees and future combined operating license applicants.

To resolve the differences between Regulatory Guide 1.152 and NEI 04-04, the TWG conducted a "gap" analysis to identify areas where the two documents overlapped or were inconsistent. The gap analysis concentrated on Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 and the programmatic elements of NEI 04-04, Rev 1. The TWG also reviewed previously-issued cyber security guidance to identify any other possible areas of inconsistency.

The TWG met with industry representatives on May 8, 2007, to review the gap analysis. The ensuing discussion and review of the gap analysis revealed that no major inconsistencies existed between the two documents. Rather, the TWG found that Regulatory Guide 1.152 was complementary to NEI 04-04 Rev. 1 on the subject of cyber security related to safety systems.

Although no major inconsistencies were revealed between the two documents, the TWG determined that there was overlapping guidance in a few programmatic areas. The industry suggested addressing the overlapping guidance to alleviate confusion going forward. Accordingly, NEI offered to revise NEI 04-04 to minimize the possibility of misinterpretation and to provide clarification with respect to the cyber security guidance for safety-related instrumentation and control systems. Following the revision, the document would be resubmitted to the NRC staff for review.

NEI also suggested that, following the review of the revised NEI 04-04, the NRC staff should provide written direction that would allow the use of either Regulatory Guide 1.152 or NEI 04-04, but not both with respect to the cyber security guidance for safety-related instrumentation and control systems. Though the staff agreed that the proposed modifications to NEI 04-04 would

help to minimize confusion going forward, it was nonetheless viewed as a sub-optimal solution for the long-term. The staff further noted that because of the likelihood of changes in this area due to emerging threats and advances in technology, regulatory guidance to address these changes would also need to be modified, necessitating changes to NEI 04-04. As such, the NRC staff did not consider NEI 04-04 to be an appropriate long-term repository for such guidance, but rather stated that a new Regulatory Guide would be developed to address cyber security defense measures required by 10 CFR 73.1 and the proposed new 10 CFR 73.55(m). In the meantime, the TWG acknowledged that NEI would submit a revision to NEI 04-04 consistent with the foregoing discussion as a short-term solution.

NEI submitted NEI 04-04 Rev. 2 to the TWG on August 6, 2007. The TWG met with industry representatives on August 17, 2007 to review the changes made to NEI 04-04 Rev. 2 and determine if the modifications made to the document were adequate to allow its use in lieu of guidance provided within Regulatory Guide 1.152 Regulatory Positions 2.1-2.9. During the discussions, concerns were identified by NRC staff regarding the ability to directly correlate the topical elements embodied within Regulatory Positions 2.1-2.9 to the programmatic guidance provided within NEI 04-04 Rev. 2. The NRC staff maintained that a strong correlation must exist between the two programs to ensure that submittals provided by licensees, permit holders, and applicants using NEI 04-04 Rev. 2 when designing, constructing, implementing or upgrading safety-related digital instrumentation and control systems did not result in adverse effect when compared to the guidance provided within Regulatory Guide 1.152.

As a result of the additional discussions with the NRC staff, NEI agreed to provide a cross-correlation table to the TWG that demonstrated how the topical elements within Regulatory Positions 2.1-2.9 mapped directly to that of requirements stated within NEI 04-04. NEI also indicated that it would resubmit an updated version of NEI 04-04 Rev. 2 along with the cross-correlation table. NEI submitted an updated version of NEI 04-04 Rev. 2 to the TWG on September 05, 2007. A cross-correlation table was also submitted to the TWG on September 06, 2007.

The TWG met once again with industry representatives on September 10, 2007 to deliver the results of its review of the previously submitted material. The NRC staff indicated that while the changes incorporated into the updated version of NEI 04-04 Rev. 2 were considered satisfactory, the cross-correlation table provided required additional information to adequately demonstrate how the topical elements within Regulatory Positions 2.1-2.9 mapped directly to the programmatic guidance stated within NEI 04-04. Further, the NRC staff noted that direction needed to be included in the cross-correlation table that unambiguously stated what specific documentation related to cyber security was expected to be provided by a licensee or applicant when submitting safety system designs for staff review. The staff considered this direction to be essential in order to ensure that reviews of submissions using NEI 04-04 Rev. 2 in lieu of Regulatory Positions 2.1-2.9 did not result in an unnecessary increase of requests for additional information by the staff, thereby needlessly extending review schedules.

At the conclusion of the meeting, the NRC staff agreed to provide the necessary corrections and additions to the supplied cross-correlation table.

A final meeting was conducted between the TWG and industry representatives on October 25, 2007 to review the finalized cross-correlation table and present the NRC staff position regarding the use of NEI 04-04 Rev. 2 in lieu of Regulatory Guide 1.152 Rev. 2, Regulatory Positions 2.1-2.9.

DRAFT

Staff Position:

The original issue brought forth by the industry asserted that Regulatory Positions 2.1-2.9 provided within Regulatory Guide 1.152 Rev. 2 conflicts with NEI 04-04 Rev. 1 with regard to the protection of safety-related digital instrumentation and control systems. However, through the TWG the NRC staff has illustrated that the programs are complementary to each other.

The guidance provided within Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2 describes, in general, an acceptable method that can be used by licensees or applicants to assist in the protection of digital computers used within safety systems from cyber threat. The NRC staff recognizes that alternative approved methods may be employed by licensees to achieve an identical effect. The staff is also sensitive to the fact that the industry is interested in pursuing efficient implementation of cyber security enhancements through the utilization of existing programs where possible.

Pending the formal acceptance of NEI 04-04 Rev. 2 by the U.S. Nuclear Regulatory Commission, licensees, permit holders, and applicants involved in the design, construction, implementation, or upgrade of safety-related digital instrumentation and control systems in nuclear power plants, should adhere to the guidance contained within Regulatory Guide 1.152 Rev. 2.

Following the formal acceptance of NEI 04-04 Rev. 2 and until the NRC provides additional guidance on this subject, licensees, permit holders, and applicants involved in the design, construction, implementation, or upgrade of safety-related digital instrumentation and control systems in nuclear power plants, who adhere to the programmatic guidance and recommendations set forth in NEI 04-04 Rev. 2 may use this program in lieu of Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2 provided that additional guidance and the submittal requirements specified in Appendix A of this ISG are followed.

Licensees permit holders and applicants are still required to identify, consider, and address all other applicable regulations, standards, and guidance when designing, constructing, implementing and upgrading digital safety systems. This NRC staff position is limited to the applicability of Regulatory Positions 2.1-2.9 found in Regulatory Guide 1.152 Rev. 2. No extrapolation or extension of this concept is inferred, approved or authorized for any other portion of Regulatory Guide 1.152 Rev. 2.

Rationale:

Based upon the results of the gap analysis performed and the lack of definitive evidence to the contrary, the TWG has determined that no major inconsistencies exist between Regulatory Guide 1.152 Rev. 2 and NEI 04-04 Rev. 1. Conversely, analysis indicates that the guidance provided in Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2 complements the industry-generated programmatic guidance contained within NEI 04-04 Rev. 1.

NEI 04-04 Rev. 2 submitted by the industry provides further clarification from a programmatic perspective regarding the protection of safety systems from cyber threat. Although NEI 04-04 Rev. 2 is similar in goal to that of Regulatory Guide 1.152 Rev. 2, the context of the program is significantly different in that it is designed to address the protection of all identified critical

DRAFT

systems located within a nuclear plant, whereas Regulatory Guide 1.152 Rev. 2 is concerned solely with safety-systems. NEI 04-04 attempts to address cyber security in a holistic manner and encompasses elements and security considerations not addressed by Regulatory Guide 1.152 Rev. 2.

The TWG has reviewed NEI 04-04 Rev. 2 and finds that the modifications made by the industry amplifies the subject matter related to safety system cyber security. The specific changes made shall not be addressed in this ISG as the material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*." This updated version of NEI 04-04 Rev. 2 will be submitted to the NRC for formal review and acceptance.

Notwithstanding the modifications made to NEI 04-04 by the industry, it is the finding of the TWG that a direct correlation between Regulatory Positions 2.1-2.9 stated within Regulatory Guide 1.152 Rev. 2 to the programmatic guidance provided within NEI 04-04 Rev. 2 is not obvious. This is due in large part to the stylistic differences that exist with regard to the language employed in each of the documents. Regulatory Guide 1.152 Rev. 2 utilizes language that is more prescriptive and deterministic when compared to NEI 04-04 Rev. 2.

To reconcile the differences in language style and contextual focus and to ensure that an adverse effect does not result when using NEI 04-04 Rev. 2 in lieu of Regulatory Guide 1.152 Rev. 2 to address cyber security issues affecting safety systems, the TWG finds that a cross-correlation table that concretely and definitively maps the topical elements within Regulatory Positions 2.1-2.9 to that of requirements stated within NEI 04-04 is necessary. A cross-correlation table provides a useful aid to individuals involved in the design, construction, implementation, and upgrade of safety systems as well as to the NRC staff when analyzing and reviewing safety system submittals provided by licensees, permit holders, or applicants. The TWG has reviewed and amplified the cross correlation table provided by NEI and has determined that it sufficiently maps Regulatory Positions 2.1-2.9 to programmatic requirements contained within NEI 04-04. Additionally, the supplied cross correlation table provides guidance regarding the documents required to be submitted for review of new or upgraded safety systems. The information contained within the cross-correlation table is withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*." The cross-correlation table is attached as Appendix A of this ISG.

Recommendation:

Until further notice, this ISG should be used when developing and implementing cyber security programs or when engaging in the design, construction, implementation, or upgrade of digital safety systems in nuclear power plants.

Applicability:

This ISG is applicable to all existing nuclear power plant licensees, permit holders and applicants.

DRAFT

References:

NRC Order EA-02-026, *Interim Compensatory Measures*, dated February 25, 2002

NRC Order EA-03-086, *Design Basis Threat for Radiological Sabotage,* April 29, 2003

IEEE Standard 603-1998, *Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, July 1, 1998

IEEE Standard 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, December 19, 2003

NRC Standard Review Plan NUREG-0800, Appendix 7.1-D, *Guidance for Evaluation of the Application of IEEE STD 7-4.3.2,* March 2007

NRC Standard Review Plan NUREG-0800, Branch Technical Position 14 *Guidance on Software Reviews for Digital computer-Based Instrumentation and Control Systems,* Revision 5, March 2007

NRC Regulatory Guide 1.152, Revision 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* January 2006

Federal Register Vol. 71, No. 207, *Power Reactor Security Requirements*, October 26, 2006

NEI 04-04 Revision 1, *Cyber Security Program for Power Reactors,* November 18, 2005

NEI 04-04 Revision 2, *Cyber Security Program for Power Reactors,* August 4, 2007

NEI White Paper, *Cyber Security Guidance for Nuclear Power Plants - The Need for a Coherent Approach*, March 5, 2007

DRAFT