

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

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

Issue:

The nuclear power industry requested clarification of conflicting guidance associated with implementation of cyber security measures at nuclear power plants. Specifically, the industry asserted that certain guidance provided in 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, Rev. 1*, document with regard to the protection of safety-related digital instrumentation and control systems. Additionally, the industry requested clarification of the NRC staff's position on the "acceptance" of NEI 04-04 as a means for establishing and maintaining an effective cyber security program at nuclear power plants.

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 expectations with regard to the implementation of cyber security requirements for nuclear power plant safety systems, and to clarify what is meant by the staff's acceptance of NEI 04-04 as an effective method for maintaining a cyber security program.

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 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."

- 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 Rev. 1, *Cyber Security Program for Power Reactors*, November 2005

In a letter dated December 23, 2005, after providing considerable in-depth review and comment, the NRC staff notified the Nuclear Energy Institute (NEI) that the industry-generated document, NEI 04-04, would be 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 Rev. 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 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 Rev. 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).

- 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 Rev. 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 the requirements for securing 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 what they perceived to be inconsistencies between certain guidance provided in Regulatory Guide 1.152 and programmatic aspects of NEI 04-04. The details of these perceived inconsistencies are not described here since NEI 04-04 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 perceived inconsistencies 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 perceived inconsistencies 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. The TWG also reviewed all 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 on the subject of cyber security related to safety systems. The perceived inconsistencies originally identified by industry were due largely to misinterpretation of certain technical content within NEI 04-04. Clarification provided by one of the primary authors of NEI 04-04 eliminated the misunderstanding.

Although no major inconsistencies were revealed, the TWG determined that there was overlapping guidance in a few programmatic areas. The industry suggested consolidating 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 requirements for securing safety-related digital 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 when seeking to secure safety-related 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 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 that a new Regulatory Guide 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 reviewed the changes to NEI 04-04 and found them acceptable. The NRC staff's interim position on the application of NEI 04-04 Rev. 2 and RG 1.152 are provided below.

Staff Position:

Until such time when 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 rigidly adhere to the programmatic guidance and recommendations set forth in NEI 04-04 Rev 2, *Cyber Security Program for Power Reactors*, August 4, 2007 may address Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006, through implementation of their respective NEI 04-04 program.

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 strictly bounded 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.

Further, the NRC staff notes that NEI 04-04 Rev. 2 establishes a framework for the development, implementation and maintenance of an effective cyber security program, but does not necessarily contain or describe all of the implementing details necessary to demonstrate an ability to defend against a determined cyber attack with high assurance. The NRC plans to provide additional regulatory guidance in support of the ongoing 10 CFR 73.55(m) rulemaking to clarify the regulatory expectations related to this topic.

Viewing NEI 04-04 Rev. 2 as a programmatic framework document does not in any way diminish its importance to the industry or to the NRC. NEI 04-04 Rev. 2 represents the collective effort of a majority of industry representatives that sought to develop a means to define what elements would be essential to the construction of an effective cyber security

program. The NRC finds NEI 04-04 Rev. 2 to be a highly constructive and informative reference in the development of its cyber security regulations and guidance documents.

Rationale:

After providing in-depth review and comment, the NRC staff determined that NEI 04-04 Rev. 2, *Cyber Security Program for Power Reactors*, August 4, 2007, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. Further, the NRC staff has determined that the changes made within this revision adequately incorporate and address Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006.

Nonetheless, the NRC staff notes that NEI 04-04 Rev. 2 does not establish minimum standards of acceptable risk and lacks the specific measures needed to mitigate such risks. In addition, NEI 04-04 does not establish quantifiable metrics to enable a meaningful assessment of cyber security program effectiveness. Due to its performance-based (i.e., non-prescriptive) nature, NEI 04-04 does not provide the type of directive statements typically found within NRC regulatory guidance documents. As such, NEI 04-04 leaves licensees and applicants open to develop their own criteria and standards. The NRC staff is concerned that this lack of specificity will result in standards that are inconsistently determined and applied throughout the industry. As such, the staff plans to develop a Regulatory Guide, in support of the ongoing 10 CFR 73.55(m) rulemaking effort, to assist licensees, permit holders, and applicants in understanding *how* to meet the acceptable standards.

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.

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, *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*

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

NRC Regulatory Guide 1.152, Rev. 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 Rev. 1, *Cyber Security Program for Power Reactors*, November 18, 2005

NEI 04-04 Rev. 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