CYBER SECURITY IN DIGITAL INSTRUMENTATION AND CONTROLS
Interim Staff Guidance-XX

Interim Resolution to Address Concerns Regarding Programmatic Implementation of Cyber Security Requirements for Nuclear Power Plants

Issue:

The nuclear power industry has requested clarification to an issue associated with the implementation of cyber security at nuclear power plants. The concern is that conflicting guidance exists for the implementation of cyber security requirements at nuclear power plants. Specifically, the industry has asserted that guidance provided under Regulatory Guide 1.152 Revision 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* conflicts with an industry developed program NEI-04-04 *Cyber Security Program for Power Reactors, Rev 1* with regard to the protection of safety-related systems. Additionally, as an ancillary development that occurred during the examination of the above issue the Industry also requested further clarification regarding the NRC staff position on the acceptance of NEI-04-04 as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants.

The above issue is addressed in this Interim Staff Guidance (ISG).

Purpose:

To clarify the NRC Staff's expectations with regard to the implementation of cyber security requirements for safety systems at nuclear power plants. Further, this ISG will clarify the Staff position regarding the acceptance of NEI-04-04 as an effective method for maintaining a cyber security program at nuclear power plants.

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:

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

  NRC Order EA-02-026 specified numerous interim compensatory measures to address the elevated threat environment. Part of this Order contained cyber security requirements that required nuclear power plants to identify digital systems that were critical to the operation of the facility, and to identify potential consequences to the facility if these systems were 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."

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

  This Order revised the Design Basis Threat (DBT) for nuclear power plants specified in 10 CFR 73.1 based in part upon information provided by the intelligence community. 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 2002, the NRC engaged Pacific Northwest National Laboratory (PNNL) to develop a cyber security self-assessment method that could be used by licensees to systematically assess the risk to systems deemed to be critical to the operation of nuclear power plants. The method was developed utilizing a multidisciplinary team from PNNL with input provided from the NRC and nuclear power industry personnel. The material aspects of NURE/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

  On December 23, 2005, after providing considerable in-depth review and comment, the NRC staff notified 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 Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Rev 2* January 2006

  Regulatory Guide 1.152 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 requirements for cyber security actions at nuclear power plants in 10 CFR 73.55 (m). The proposed rule maintains the intent of the previously issued security orders (EA-02-026 and EA-03-086) and requires licensees to implement a cyber security program to detect and prevent cyber attacks on plant computer systems.

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

  BTP 7-14 provided guidelines for evaluating software life-cycle processes for digital computer-based instrumentation and control (I&C) systems for nuclear power plants. It addresses characteristics that should be present within an acceptable Software Management Plan that the licensee should provide a description of the methods to be used to prevent corruption of the developed software by viruses, Trojan horses or other nefarious intrusions. The required security level for each project phase should be identified.

- *72 Federal Register 12705 Final Rule on the Design Basis Threat (DBT), published March 19, 2007*

  This final rule on the DBT includes a provision for licensees to protect against "cyber attacks."

Discussion:

As the nuclear power industry engaged in the process of identifying and implementing enhancements to cyber security in order to further secure their facilities from cyber threats, uncertainty developed within the industry as to which program(s) bore precedence when attempting to secure safety systems. Specifically, the industry identified what they perceived to be inconsistencies between the guidance provided within Regulatory Guide 1.152 and programmatic aspects of NEI 04-04. The details of these perceived inconsistencies are not delineated within this ISG 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 and discussed methods to resolve perceived inconsistencies between the various guidance documents pertaining to cyber security of power reactors. In response to the concerns raised by the industry, a Task Working Group (TWG) was established to address cyber security issues related to Digital Instrumentation and Controls (DI&C). The primary objective of the TWG was to ensure that the cyber security guidance provided was coherent and consistent for existing licensees as well as future Combined License Applicants that may be proposing plant-specific DI&C systems.

To resolve the perceived inconsistencies between Regulatory Guide 1.152 and NEI 04-04, the NRC staff 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 programmatic elements of NEI-04-04. The NRC staff also reviewed all previously issued guidance regarding cyber security to identify other possible areas of inconsistency.

The TWG held a meeting on May 8, 2007, to review the NRC’s 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 to misinterpretation of technical content that existed within NEI-04-04. Clarification provided by one of the primary authors of NEI-04-04 eliminated the misunderstanding that caused the misinterpretation.

Although the review indicated that no major inconsistencies existed, the TWG observed that overlapping guidance did exist in a few programmatic areas. The industry suggested consolidating the overlapping guidance to alleviate confusion going forward. NEI offered to revise NEI 04-04 to eliminate the possibility of misinterpretation regarding Issue 1 of this ISG while also offering to provide amplification in the area of securing safety systems. Following the revision, the document would be resubmitted to the NRC staff for review and subsequent acceptance. If found acceptable, NEI suggested that direction could be provided by the NRC staff that Industry could be allowed to choose to follow either Regulatory Guide 1.152 or NEI-04-04 when seeking to secure safety-related digital I&C systems.

The NRC staff responded that although the offer to incorporate further guidance into NEI-04-04 would help to alleviate the immediate issue (Issue 1), it was viewed as untenable as a long-term solution. The staff indicated that regulatory requirements would likely experience change in this area due to emerging threats, changes in cyber attack vectors, changes in technology, as well as changes in mitigation tools and techniques. Such changes in regulatory requirements would inevitably lead to the need to provide additional guidance to assist the industry in meeting the regulations. The NRC staff did not consider NEI 04-04 to be the appropriate long-term repository for such guidance.

The foregoing TWG dialogue led to the development of Issue 2 described within this ISG. Specifically, the Industry requested that the NRC staff further clarify its position regarding what the "acceptance of NEI-04-04" meant from a regulatory perspective. The NRC staff agreed to respond to the request. The TWG adjourned with an agreement that NEI would submit a revision to NEI-04-04 to eliminate the possibility of misinterpretation of Issue 1. The NRC staff agreed to review the proposed changes to NEI-04-04 and if found to be acceptable, consider the impact of those changes when providing resolution to the issues identified in this ISG.

Staff Position on Issue:

Until such time when the NRC provides additional guidance on the subject, licensees and permit holders as well as Combined License Applicants involved in the design, construction, implementation, or upgrade of digital safety systems in nuclear power plants who voluntarily implement and rigidly adhere to the programmatic guidance and recommendations set forth in NEI 04-04, *Cyber Security Program for Power Reactors, Rev 2, Month Day*, 2007 may address Regulatory Positions 2.1-2.9 found in *Regulatory Guide 1.152 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", Rev 2 January 2006,* through implementation of their respective NEI-04-04 program.

Licensees and Combined License 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 interim staff position is strictly bounded to the applicability of Regulatory Positions 2.1-2.9 found in

Regulatory Guide 1.152. No extrapolation or extension of concept is inferred, approved or authorized for any other portion of Regulatory Guide 1.152.

As to the NRC staff position on the acceptance of NEI-04-04, the staff agrees that the core components within NEI 04-04 define the content of an effective cyber security program. NEI 04-04 defines a framework for the creation and maintenance of a cyber security program but not necessarily all of the implementing details needed to demonstrate high assurance for protecting against a cyber attack. As such, industry should expect that the NRC will provide regulatory guidance in support of the 10 CFR 73.55 rulemaking. This will clarify the NRC's expectations on this topic.

Viewing NEI 04-04 as a programmatic framework document does not in any way diminish its importance to the industry or to the NRC. NEI 04-04 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 that the industry could use as a model. The NRC finds NEI 04-04 to be a constructive and informative reference point in the development of its regulations and guidance associated with cyber security.

Rationale:

NEI-04-04 does not establish minimum standards of acceptable risk and lacks 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 the performance-based (i.e., non-prescriptive) nature of NEI 04-04, it does not provide the type of directive statements typically found within NRC regulatory guidance. NEI-04-04 leaves the licensee to develop its own criteria and standards. The NRC staff is concerned that this lack of specificity will result in standards that are inconsistently determined and indiscriminately applied throughout the industry. The NRC needs to ensure that recognized standards are applied consistently throughout the industry and will develop, as necessary, Regulatory Guides to assist licensees and applicants in understanding *how* to acceptably meet the standards.

After providing in-depth review and comment, the NRC staff determined that NEI 04-04, "Cyber Security Program for Power Reactors," Revision 2, dated Month, Day, 2007, remains 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 the revision adequately incorporate and programmatically address Regulatory Positions 2.1-2.9 existing within *Regulatory Guide 1.152 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", Rev 2 January 2006.*

Recommendation:

Until further notice, this ISG should be used by existing licensees and Combined Operating License Applicants 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 current licensees of nuclear power plants and Combined Operating License Applicants.

References:

EA-02-026, “Interim Compensatory Measures (ICM) Order,” dated February 25, 2002

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

U.S. Nuclear Regulatory Commission Standard Review Plan NUREG-0800, Appendix 7.1-D, *Guidance for Evaluation of the Application of IEEE STD 7-4.3.2*

U.S. Nuclear Regulatory Commission Standard Review Plan NUREG-0800, Branch Technical Position HICB-14, *Guidance on Software Reviews for Digital computer-Based Instrumentation and Control Systems*

U.S. Nuclear Regulatory Commission Regulatory Guide 1.152, Rev 2, January 2006 *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*

“Power Reactor Security Requirements,” Federal Register /Vol. 71, No. 207 / Thursday, October 26, 2006

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

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