June 8, 2011

Dr. Said Abdel-Khalik, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: RESPONSE TO ADVISORY COMMITTEE ON REACTOR SAFEGUARDS RECOMMENDATIONS ON DRAFT FINAL REVISION 3 OF REGULATORY GUIDE 1.152,"CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS"

Dear Dr. Abdel-Khalik:

In your letter dated April 20, 2011 (Agencywide Documents Access and Management System Accession No. ML11101A013), you summarized the views of the Advisory Committee on Reactor Safeguards (ACRS or the Committee) with respect to draft final Revision 3 of Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." The staff of the U.S. Nuclear Regulatory Commission (NRC) is committed to working closely and cooperatively with the Committee to resolve ACRS recommendations when this will improve the regulatory process.

This letter responds to the five recommendations in your letter. The staff will revise RG 1.152 and the standard review plan (SRP) to address Recommendations 4 and 5. Recommendations 1, 2, and 3, will be incorporated into RG 1.152, to the extent the recommendations are consistent with the regulations. The existing regulatory framework protects against safety and security concerns for digital safety systems without needing rulemaking, as would be necessary to fully implement the Committee's proposed revisions.

The ACRS's recommended approach prescribes that a finding be made by the staff on the effectiveness of cyber security measures during the licensing review of the design. While this provides a certain level of confidence early, it could generate a false sense of confidence given the evolving nature of cyber-based threats, and may be less effective in the long run when compared to our current performance based approach. The strength of the current approach is that it provides the necessary flexibility to address the dynamic nature of the cyber threat. The current approach appropriately places the responsibility of maintaining effective cyber security protection on licensees and applicants.

On the basis of discussions during meetings with the ACRS, the staff recognizes the concern that there is risk in evaluating compliance via inspection later in the system lifecycle rather than relying on the licensing review early in the system lifecycle. In the event a licensee or the NRC identifies a cyber vulnerability that cannot be addressed through their programmatic defensive measures, as may have been originally planned by that applicant or licensee, a license amendment request may be necessary to change the design. At the ACRS subcommittee meeting on Revision 3 to RG 1.152 in February 2011, licensee representatives told ACRS

members that licensees understand that they are responsible for safety and security of digital safety systems throughout the life cycle of the systems. This approach appropriately puts this risk on the entities responsible for ensuring their systems are secure.

ACRS Recommendation 1:

Draft Final Revision 3 of RG 1.152 should not be issued until Recommendations 2, 3, and 4 are incorporated.

NRC Response:

The staff has revised draft final Revision 3 of RG 1.152 to incorporate Recommendation 4 as described below. As discussed below, the staff plans to issue Revision 3 of RG 1.152 in late June 2011, following review by the Office of the General Counsel, without fully incorporating the revisions recommended in Recommendations 2 and 3.

ACRS Recommendation 2:

RG 1.152, Revision 3, Regulatory Position 2.3, "Design Phase," should be revised to reference RG 5.71 and state that digital safety system designs should incorporate hardware and software architectures capable of providing a cyber security defensive architecture to combat malicious cyber security threats.

NRC Response:

The ACRS proposal to incorporate cyber security evaluations as part of safety reviews is inconsistent with existing regulations since Title 10 of the *Code of Federal* Regulations (10 CFR) Part 50.55(a) does not require incorporation of cyber security features. However, the staff will revise RG 1.152 to provide an appropriate pointer to the provisions of 10 CFR 73.54 "Protection of digital computer and communication systems and networks," and RG 5.71 that address cyber security defensive architecture into the discussion section of RG 1.152, Revision 3, to include the following:

> Licensees should be aware that digital safety systems will be considered Critical Digital Assets and must adhere to the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks." Regulatory Guide 5.71 describes an acceptable defensive architecture to comply with 10 CFR 73.54. The architecture described in the guidance would have licensees place all digital safety systems in the highest level of their defensive architecture and only permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture. Licensees should be aware that Section B.1.4 of Appendix B to Regulatory Guide 5.71 notes that one-way communications should be enforced using hardware mechanisms. A licensee's adherence to the provisions of 10 CFR 73.54 will be evaluated per regulatory programs specific to that regulation.

ACRS Recommendation 3:

Explicit statements that the licensing design reviews will not address cyber security design features for other than their effect on the safety system should be deleted. Licensees should understand that as part of the safety system review, all features of their designs will be reviewed for licensing purposes, including cyber security, to the extent possible.

NRC Response:

The staff does not intend to implement ACRS Recommendation 3, because it is inconsistent with the existing regulatory framework. The staff will retain the language of RG 1.152, Revision 3 to ensure consistency with 10 CFR 73.54 which is a performance-based regulation. The 10 CFR 73.54 contains language that precludes detailed review of cyber security features during licensing. A more detailed discussion of the existing regulatory framework and associated guidance is contained in the Discussion section of this letter.

ACRS Recommendation 4:

If the staff cannot provide hazard identification guidance for acceptable methods, RG 1.152 Regulatory Position 2.1, “Concepts Phase,” should be revised to state that, while Annex D of IEEE Standard 7-4.3.2-2003 is not endorsed by the NRC, the hazard identification guidance in Annex D may provide useful information on the assessment of the susceptibility of safety systems to inadvertent access.

NRC Response:

The staff will amend the Discussion section of RG 1.152 to address Annex D of Institute of Electrical and Electronics Engineers (IEEE) 7-4.3.2-2003 in this fashion.

ACRS Recommendation 5:

The Standard Review Plan (SRP) for Chapters 7, “Instrumentation and Controls,” and 13, “Conduct of Operations,” should formally require internal staff coordination of reviews to RGs 1.152 and 5.71 during the system design reviews.

NRC Response:

The staff is currently developing an interoffice instruction that would address the interactions between the Office of Nuclear Reactor Regulation (NRR), the Office of New Reactors (NRO), the Office of Nuclear Security and Incident Response (NSIR), and the regional offices in reviewing digital safety systems and their cyber security provisions. Additionally, at the next planned update of SRP Chapters 7 and 13, the staff will add language to define where the safety and security reviews will be completed and to provide the appropriate references to staff reviews and inspections that will be completed as part of the staff evaluation under other chapters. These staff documents will discuss the interfaces needed to support these reviews, the information that is to be provided, and when in the review process these staff interfaces should occur.

Discussion:

The process for reviewing digital instrumentation and control systems associated with plant safety, as discussed in draft final RG 1.152, Revision 3, currently focuses on the establishment of secure development and operational environments (SDOE) for digital safety systems. During digital safety system licensing reviews, the staff focuses on ensuring that the development environment for the digital safety system is secure from the introduction of unwanted, unneeded, and undocumented code and the staff will evaluate the controls placed on the development environment. In addition, staff guidance and licensing criteria ensure that a secure operational environment for digital safety has been established. During licensing reviews, the staff verifies that a licensee's secure operational environment provides protection from undesirable behavior from connected systems and from inadvertent access to the digital safety system. The staff evaluates the adequacy of the design provisions to address the identified undesired behaviors and verify that the design features were appropriately addressed throughout the development process. The staff also evaluates the adequacy of the provisions and associated supporting design features to preclude inadvertent access to the system.

The staff understands the Committee's desire to have cyber security design evaluated during licensing reviews. However, 10 CFR 73.54 (the cyber security rule) is a performance-based regulation that focuses on measurable outcomes and defined results rather than prescriptive processes, techniques, procedures, or specific direction on the means for obtaining those results. Given the constantly evolving nature of cyber-based threats, this affords licensees more flexibility in determining the means for meeting those outcomes. For licensing, 10 CFR 73.54 requires licensees and combined operating license (COL) applicants to submit cyber security plans (CSPs) for the NRC's review and approval. The CSPs submitted by licensees and applicants, which were consistent with the CSP template provided in RG 5.71, contain sufficient information to support NRC staff reviews throughout the 10 CFR 73.54 licensing process.

Given the agency's programmatic approach to cyber security, 10 CFR 73.54(f) contains the following language that endorses the concept that the technical details of cyber features will not be reviewed in licensing:

> The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

The staff has incorporated this approach into RG 5.71, including in the following citation:

> If a licensee or applicant chooses to address 10 CFR 73.54 though the use of design features, then details of any design features of the safety system, intended to meet a cyber security provision of 10 CFR 73.54, must be submitted as part of the license amendment request or design certification application or COL application for review and approval. In such cases, the NRC will review those features only in conjunction with the system's safety functions to ensure that the reliability of the safety system is not adversely impacted by the inclusion of these security features.

Interim Staff Guidance DI&C-06 states the following:

> Any cyber security design features included as part of a safety system for the purposes of complying with 10 CFR 73.54 would be reviewed to ensure that their inclusion would not impact the reliable performance of the safety function. However, no evaluation of the adequacy of those cyber security features should be made as part of the licensing review.

The staff has also incorporated the approach into draft final RG 1.152, Revision 3:

> For licensees that choose to provide, as part of their license submittal, descriptions of cyber-security design features intended to address the guidance of RG 5.71, the extent of the staff's review of these features is limited to ensuring that these features do not adversely affect or degrade the system's reliability or its capability to perform its safety function.

As stated in RG 1.152, Revision 3, the NRC staff will review cyber security design features within a digital safety system, but the safety system licensing review will be limited to ensuring that the cyber security features do not degrade the reliability or performance of the digital safety system. Any design provisions of a digital safety system that are intended to serve both SDOE and cyber security functions would only be evaluated as part of the digital safety system licensing review for their ability to satisfy the SDOE functions. This approach is consistent with 10 CFR 73.58, "Safety/security interface requirements for nuclear power reactors," that requires licensees to assess and manage the potential for adverse effects on safety and security before implementing changes to plant configurations, facility conditions, or security. The regulation at 10 CFR 73.58 further requires licensees to take appropriate compensatory or mitigating actions to maintain safety and security where potential conflicts are identified. Once the NRC approves the digital safety system through the 10 CFR Part 50 or 10 CFR Part 52 licensing process, licensees or applicants are required to protect the system from cyber security threats by satisfying the provisions of 10 CFR 73.54. Under these provisions and as a condition of its license, each licensee must submit a CSP to the NRC for review and approval. The evaluation of any specific cyber security feature or controls to meet 10 CFR Part 73, "Physical Protection of Plants and Materials," would be in the domain of the NRC's inspection programs.

The staff will retain the language in RG 1.152, Revision 3, that indicates that evaluation of cyber security provisions for their ability to thwart cyber security threats will fall under the staff's cyber security inspection program and will not be performed as part of the licensing reviews under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."

Although the licensing reviews associated with 10 CFR Part 50 and 10 CFR Part 73 requirements are completed separately, it should be noted that the consideration for the security/safety interface is part of the regulatory review process for all license amendment and initial applications, and consistent with the requirements in 10 CFR 73.58 as previously noted. As part of the staff's response to a Staff Requirements Memorandum dated April 8, 2004, NRR, NRO, and NSIR established office procedures to ensure that licensees take an integrated approach to developing and implementing proposed changes as part of license amendments or applications, and that the NRC uses an integrated safety/security interface.

Licensing reviews performed under 10 CFR Part 73 will evaluate whether commitments made by licensees and applicants within their prospective CSPs include those cyber security-related provisions necessary to ensure that digital safety systems are adequately protected against cyber attacks, up to and including the design-basis threat, throughout each phase of the system life cycle. For example, cyber security provisions pertaining to the development phase of a digital safety system that are outlined in the licensee's or applicant's CSPs include requirements specifying that developers will (1) maintain the integrity of the systems until the product is delivered to the licensee, (2) employ software quality and validation methods to minimize flawed or malformed software, (3) ensure that the developed systems have the capability to address security controls provided in the license conditions, and (4) ensure that developed systems are free from known, testable vulnerabilities and malicious code. Provisions in the CSPs also call for licensees and applicants to verify and validate the proper performance of these actions.

The staff is currently developing inspection procedures and associated guidance for the NRC cyber security oversight program. The purpose of this inspection program will be to ensure that requirements for the secure operation of digital safety systems at a nuclear power plant, as described in licensee and applicant CSPs, are met (before the arrival of fuel on site for new plant applicants). In addition, the staff is also strengthening internal coordination between offices through the development of interoffice procedures to ensure that 10 CFR Part 50, 10 CFR Part 52, and 10 CFR Part 73 licensing reviews and inspections are coordinated appropriately.

After incorporating the changes discussed above, the final RG 1.152, Revision 3, will be issued as it is consistent with the existing regulatory framework. The current regulatory structure adequately addresses safety and security issues. The staff appreciates the comments and recommendations provided by ACRS. We look forward to continuing to work with the Committee.

Sincerely,

/RA by Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

Licensing reviews performed under 10 CFR Part 73 will evaluate whether commitments made by licensees and applicants within their prospective CSPs include those cyber security-related provisions necessary to ensure that digital safety systems are adequately protected against cyber attacks, up to and including the design-basis threat, throughout each phase of the system life cycle. For example, cyber security provisions pertaining to the development phase of a digital safety system that are outlined in the licensee's or applicant's CSPs include requirements specifying that developers will (1) maintain the integrity of the systems until the product is delivered to the licensee, (2) employ software quality and validation methods to minimize flawed or malformed software, (3) ensure that the developed systems have the capability to address security controls provided in the license conditions, and (4) ensure that developed systems are free from known, testable vulnerabilities and malicious code. Provisions in the CSPs also call for licensees and applicants to verify and validate the proper performance of these actions.

The staff is currently developing inspection procedures and associated guidance for the NRC cyber security oversight program. The purpose of this inspection program will be to ensure that requirements for the secure operation of digital safety systems at a nuclear power plant, as described in licensee and applicant CSPs, are met (before the arrival of fuel on site for new plant applicants). In addition, the staff is also strengthening internal coordination between offices through the development of interoffice procedures to ensure that 10 CFR Part 50, 10 CFR Part 52, and 10 CFR Part 73 licensing reviews and inspections are coordinated appropriately.

After incorporating the changes discussed above, the final RG 1.152, Revision 3, will be issued as it is consistent with the existing regulatory framework. The current regulatory structure adequately addresses safety and security issues. The staff appreciates the comments and recommendations provided by ACRS. We look forward to continuing to work with the Committee.

Sincerely,

/RA by Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

DISTRIBUTION: G20110285/EDATS: OEDO-2011-0280 RidsNsirOd RidsNrrOd
RidsAcrsAcnw_MailCTR RidsNrrMailCenter RidsEdoMailCenter RidsNroDe
RidsResOd RidsOgcMailCenter RidsNrrDe

ADAMS Accession Nos.: Pkg: ML111380685 Incoming: ML11112A140; Ltr; ML111390059; *Via email

OFFICE:	NRR/DE	NRR/DE	Tech Ed.	NRR/DE	NRR/DE
NAME:	TMossman	SArndt	KAzariah-Kribbs	GWilson	PHiland
DATE:	05/19/2011	05/19/2011	05/18/2011	05/18/2011	05/20/2011
OFFICE:	NRO/DE	NRO	NSIR	NSIR	NRR
NAME:	TBergman	MJohnson	MLayton	JWiggins	ELeeds(WRuland for)
DATE:	06/01/2011	06/01/2011	06/01/2011	06/02/2011	06/03/2011
OFFICE:	EDO				
NAME:	RBorchardt				
DATE:	06/8/ 2011				

OFFICIAL RECORD COPY