March 25, 2010

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

SUBJECT: DRAFT FINAL REGULATORY GUIDE 5.71, "CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES"

Dear Dr. Abdel-Khalik:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to the November 12, 2009, letter from the Advisory Committee on Reactor Safeguards (ACRS) Chairman Mario Bonaca to Chairman Gregory B. Jaczko. The letter summarized the views of the ACRS on the Draft Final Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities." The NRC staff generally agrees with the recommendations in the letter as discussed below.

ACRS Recommendation 1

RG 5.71 should be issued to support compliance with 10 CFR 73.54.

NRC Response

The staff agrees. Regulatory Guide 5.71 was issued in final form on January 7th, 2010.

ACRS Recommendation 2

RG 5.71 adapts the National Institute of Standards and Technology (NIST) Standards for the development of plans but does not provide guidance to evaluate their adequacy.

NRC Response

The NRC staff agrees with the ACRS concern for providing licensees guidance to evaluate cyber security plan adequacy. The staff believes the approach in RG 5.71 (i.e., Appendix A, Section A.2.2) is consistent and aligned with the approach used in physical security. The physical security plan approach, which is established, maintained, and implemented by the licensee, provides for consistent, continuous reviews of the effectiveness of the security organization through performance evaluations.

The approach described in RG 5.71 incorporates performance evaluation testing with effectiveness and vulnerability analyses as noted in Sections C.3.3, C.4.1.2, and C.4.1.3. These sections describe the effectiveness analysis and vulnerability tests to be performed to provide assurance that an adversary is unable to compromise the defensive strategies for a Critical Digital Asset (CDA). The NRC staff also believes that the RG 5.71 approach, when properly implemented, will provide high assurance of adequate protection against cyber attacks

because it incorporates multiple diverse barriers and strategies for each CDA (i.e., the use of the defensive model described in Section C.3.2.1 and the use of the security controls enumerated in Appendices B and C). The staff plans to investigate if security control attributes provide performance measures for the degree of adversarial penetration and to review the possibility of developing an overall performance indicator.

ACRS Recommendation 3

After the initial implementation of the cyber security plans, RG 5.71 should be revised to include the resulting insights and to provide guidance regarding the adequacy of cyber security plans and policies.

NRC Response

The staff agrees and plans to revise RG 5.71 as needed based on insights gained from the licensing reviews of site-specific cyber security plans, licensee deployment and use of the cyber security plans and programs, industry feedback, and site-specific inspection results. Moreover, licensees are expected to modify their security programs as a result of continuous monitoring activity and assessment as stated in section C.4 (i.e., when weaknesses are indentified or new vulnerabilities are discovered).

ACRS Recommendation 4

Longer-term research projects should be initiated by the Office of Nuclear Regulatory Research (RES) in the following areas:

- Exploration of the use of probabilistic risk assessment (PRA) insights in cyber security, particularly those regarding accident sequences.

- Development of better guidance on the interaction between cyber security and safety.

- Investigation of supply chain attacks.

NRC Response

The long-term research topics recommended for inclusion are covered in ongoing and planned research programs in the NRC's Digital System Research Plan FY 2010 – FY 2014, which was recently reviewed by the ACRS. The only exception is the supply chain attacks topic; that is being considered in a collaborative exploration effort with the Department of Homeland Security and other Federal agencies.

As for the exploration of the use of PRA insights in cyber security, the NRC staff agrees with the ACRS that a plant-specific PRA identifies the accident sequences that may lead to core damage and that PRAs can be useful tools for licensees to use (along with other plant documentation and tools) in the identification of critical systems and CDAs. Referring to the ACRS statement that "A successful cyber attack would have to trigger one of these (accident) sequences," we agree this would be a primary concern. However, we would like to clarify that the focus of cyber security is to prevent and/or mitigate deliberate malicious actions, whereas PRAs and their associated accident sequences are based on traditional equipment failures and probabilities.

The cyber security strategic approach in RG 5.71 assumes the variability of possible attack vectors because the malicious threat is constantly evolving and requires constant monitoring for new threats. The staff further believes that system failures modeled in PRAs represent only a subset of the possible consequences of malicious activities (e.g., an entirely new failure mode may result, not simply "failure to start" or "failure to actuate"). Malicious actions can include the loss of control of a system, loss of integrity, loss of confidentiality, data tampering, social engineering, or degradation of system operation.

Risk assessment of complex combinations of malicious actions will need to build upon digital PRA development. The updated Research Plan addresses this need with both the Digital System PRA and the Analytical Assessment of DI&C Systems research program areas.

The development of better guidance on the interaction between cyber security and safety is a continuing concern, and the NRC staff is presently updating RG 1.152, "Criteria for Safety Systems of Nuclear Power Plants," to clarify safety system design guidance in light of the newly issued cyber security guidance. The staff understands this interaction between cyber security and safety issue is dynamic, and RES will continue to respond to specific Office of Nuclear Security and Incident Response, Office of New Reactors, and Office of Reactor Regulation needs within the existing planned research programs.

We appreciate the comments and recommendations provided by the ACRS, and look forward to continuing discussions with the Committee as the staff evaluates future updates to RG 5.71 and results of long-term research in the noted areas.

Sincerely,

/RA by Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Klein
Commissioner Svinicki
SECY

The cyber security strategic approach in RG 5.71 assumes the variability of possible attack vectors because the malicious threat is constantly evolving and requires constant monitoring for new threats. The staff further believes that system failures modeled in PRAs represent only a subset of the possible consequences of malicious activities (e.g., an entirely new failure mode may result, not simply "failure to start" or "failure to actuate"). Malicious actions can include the loss of control of a system, loss of integrity, loss of confidentiality, data tampering, social engineering, or degradation of system operation.

Risk assessment of complex combinations of malicious actions will need to build upon digital PRA development. The updated Research Plan addresses this need with both the Digital System PRA and the Analytical Assessment of DI&C Systems research program areas.

The development of better guidance on the interaction between cyber security and safety is a continuing concern, and the NRC staff is presently updating RG 1.152, "Criteria for Safety Systems of Nuclear Power Plants," to clarify safety system design guidance in light of the newly issued cyber security guidance. The staff understands this interaction between cyber security and safety issue is dynamic, and RES will continue to respond to specific Office of Nuclear Security and Incident Response, Office of New Reactors, and Office of Reactor Regulation needs within the existing planned research programs.

We appreciate the comments and recommendations provided by the ACRS, and look forward to continuing discussions with the Committee as the staff evaluates future updates to RG 5.71 and results of long-term research in the noted areas.

Sincerely,

/RA by Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Klein
Commissioner Svinicki
SECY

DISTRIBUTION: G20090650/LTR-09-0563/EDATS: SECY-2009-0511

DE r/f	ACRS File	RidsResPmdaMail	R. Borchardt, EDO
M. Virgilio, DEDMRT	B. Mallett, DEDR	D. Ash, DEDCM	N. Mamish, EDO
S. Burns, OGC	E. Leeds, NRR	J. Wiggins, NSIR	A. Frazier, EDO
M. Johnson, NRO			

ADAMS Accession No.: ML100252211

OFFICE	RES/DE/DICB	SUNSI REVIEW	RES/DE/DICB	TECH EDITOR	NSIR/DSP
NAME	K. Sturzebecher	K. Sturzebecher	R. Sydnor	J. Zabel (via email)	S. Morris
DATE	01/26/10	01/26/10	01/26/10	01/25/10	01/27/10

OFFICE	NRR/ADES/DE	NRO/DE	D: RES/DE	D: RES	EDO
NAME	D. Skeen (via email)	L. Dudes (via email)	M. Case	B. Sheron	R. Borchardt ***(M. Virgilio for)***
DATE	01/27/10	01/27/10	01/29/10	01/29/10	03/25/10

OFFICIAL RECORD COPY