UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

March 19, 2009

The Honorable Dale E. Klein
Chairman
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

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

Dear Chairman Klein:

During the 560th meeting of the Advisory Committee on Reactor Safeguards, March 5 - 7, 2009, we reviewed the Draft Final Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities" (Reference 1). Our Digital Instrumentation and Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on February 26, 2009. During these reviews, we had the benefit of discussions with representatives of the NRC staff. We also had the benefit of the documents referenced.

CONCLUSIONS AND RECOMMENDATIONS

RG 5.71 should not be published until it is revised to:

1. Provide a reference DI&C computer, communication, and network security framework that identifies assets, associated plant functions, vulnerabilities, interaction, and access pathways.

2. Include examples and more specific guidance on how the requirements of 10 CFR 73.54 can be met.

3. Ensure that the guidance distinguishes between DI&C system and non-real-time information technology system architectures.

4. Address the issues of threat assessment, dependency analysis, and the use of Probabilistic Risk Assessment (PRA) (Reference 2).

DISCUSSION

10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," requires, in part, that the licensees provide a high assurance that DI&C computers, communication systems, and networks are adequately protected against cyber attacks. RG 5.71 is intended to provide an approach that the NRC staff deems acceptable for complying with the requirements of this regulation. Such an approach would ensure consistency among licensee submittals, reviewer evaluations, and inspector activities.

The guidance in RG 5.71 is not specific enough to achieve these objectives. This Guide is a high-level document that essentially repeats the requirements stated in 10 CFR 73.54. It does not elaborate on the acceptance criteria that, when satisfied, would provide high assurance of adequate protection against cyber attacks.

During the February 26, 2009, Subcommittee meeting, representatives of the staff and Nuclear Energy Institute (NEI) stated that there were three main reasons for the conscious choice of leaving the content of the Guide at the current high level:

- Sensitivity to public disclosure of detailed information concerning nuclear power plant systems.

- Rapidly changing nature of digital technology that may bring along an equally rapidly changing nature of the security threats.

- Preference for performance-based regulatory criteria limited in prescriptive content.

Although we agree with these concerns in principle, we offer the following comments:

- There are ways of addressing the sensitivity issue. For example, a generic reference framework for cyber security could be described in RG 5.71 that would specify the required information and level of analysis that a licensee should provide. This framework could be defined in sufficient detail and scope to serve as guidance for the licensee submittal are without disclosing specific facility and system details.

- It is true that the digital and network technology is changing at a rapid pace. However, this change does not affect significantly the internal functional environment of digital controls and data pathways that are of concern for a typical plant.

- The performance requirements stated in this Guide are not numerical as, for example, those in the Maintenance Rule. They simply identify the types of strategies to be provided for compliance. In this case, a description of a minimum threshold of quality and information content of such strategies is needed.

The starting point for the development of specific guidance would be to define a generic framework for security that could help define the minimum technical attributes regarding:

- the critical digital assets (CDAs),
- the associated functions,
- asset interactions and pathways,
- infrastructure services that support the CDAs,
- defensive measures that address the cyber security threats,
- the consequences of an intrusion, and
- protective provisions.

In our report dated April 29, 2008, (Reference 2), we offered the following comments on the Interim Staff Guidance (ISG) on Cyber Security that preceded RG 5.71:

- A threat assessment should be performed to ensure that the defensive measures are addressing the right cyber security threats. This assessment should include both internal and external threats.

- Dependency analysis is necessary to identify plant infrastructure services (power, heating, ventilation, and air conditioning, etc.) that support CDAs. The cyber security program should protect the CDAs and ensure that their support systems and any interfacing data systems are also protected.

- The process for the identification of CDAs is expected to use insights from the plant PRA. Although we concur with this practice, we note that DI&C systems are modeled at a simplistic level in current PRAs. Therefore, any insights from the PRA regarding the risk significance of these systems should be viewed with caution.

We continue to believe that these comments should be addressed in RG 5.71. The information in the staff's presentation slides (Reference 4) provided to the Committee during its meeting on March 5, 2009, could be the basis for the development of an evaluation approach for cyber security. Regarding threat assessment, we recognize that a quantification of specific threat frequencies is difficult. However, a systematic delineation of threat scenarios (e.g., using event-sequence diagrams or other similar risk-assessment tools) is a useful method to identify vulnerabilities and pathways that could compromise CDAs, which may be overlooked without an integrated scenario context.

In addition, along with the generic reference framework, examples of characteristics of strategies and procedures that are acceptable to the NRC should be included in RG 5.71. A previous version of this Guide (DG-5022, Reference 3) contained examples within each topical area that helped define what is expected of the licensees.

An example of lack of specificity is Section 3.4.2.1, "System Hardening Program," in RG 5.71. It is stated that an acceptable method to develop a system hardening program for critical systems includes the following attributes:

- Develop system hardening program policy that defines the purpose, scope, roles, responsibilities, and management commitments to provide a high assurance that all existing critical systems are securely configured to prevent unauthorized access and use of critical systems.

- Develop procedures to facilitate and maintain system hardening policy.

The corresponding Section 3.2.2.2 in DG-5022 states that characteristics of strategies and procedures that are acceptable to the NRC staff include, but are not limited to:

- The removal of unnecessary default accounts or test accounts, file shares, operating system services and ports.

- The installation of access controls on file systems, file shares registries, executables (binaries) where possible to limit inappropriate access or misuse of the system.

- Access to the peripheral resources on a CDA should be controlled (e.g., external drives, ports (Serial/Parallel, USB- Universal Serial Bus, SCSI- Small Computer System Interface), Firewire).

- Role-based access controls should be where appropriate, and reduced to the lowest level possible to reasonably perform a user's job function.

- Monitoring and logging of logical access to critical digital systems and critical digital assets.

- Remote access or remote control to a critical digital systems and critical digital assets.

Without necessarily endorsing these specific characteristics, we find that the strategy characteristics contained in DG-5022 provide appropriate specific guidance on what would be acceptable to the staff in this topical area. In contrast, the corresponding Section in RG 5.71 simply asks that programs and procedures be developed without any guidance as to what would be acceptable.

In response to the suggestions at the February 26, 2009, Subcommittee meeting, the staff provided some examples for inclusion in RG 5.71. They consisted of two tables provided to us during our meeting on March 5, 2009, (Reference 5) identifying categories of exploitation, sample protocols and associated sample cyber security controls. However, these examples are exclusively drawn from non-real-time commercial network and communications and information technology experience. The examples should include guidance that is relevant to the unique design and physical location of the DI&C systems used for reactor protection and safeguards control. Examples of features used to provide security for such systems often include:

- They reside within the Level 4 (Vital Area) and Level 3 (Protected Area) shown in Figure 1, Cyber Security Defensive Model, of RG 5.71.

- They only communicate one way, out of their respective areas.

- They use real-time, custom software and safety qualified input/output and data transmission protocols.

- They are designed with detailed internal area configuration and access controls to protect against internal security threats.

Although RG 5.71 provides a glossary, there are some important terms that are not defined. These include: cyber-security, system integrity, information integrity, system integrity controls, and information integrity controls.

We were told by the staff that the current version of RG 5.71 is under revision and our comments will be considered. We look forward to reviewing the revised version of the RG 5.71.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

References:

1. Regulatory Guide RG 5.71, “Cyber Security Programs for Nuclear Facilities,” Nuclear Regulatory Commission, Washington, DC, January 2009 (ML090760860)

2. Letter from William J. Shack, Chairman, ACRS, to Dale E. Klein, Chairman, NRC, Subject: Digital Instrumentation and Control Systems Interim Staff Guidance, dated April 29, 2008(ML081050636)

3. Draft Regulatory Guide DG-5022, “Cyber Security Programs for Nuclear Facilities,” Nuclear Regulatory Commission, Washington, DC, December 2008 (ML090760900)

4. Slide 8 of the Staff’s Presentation Materials on RG 5.71 Cyber Security Programs for Nuclear Facilities, presented to the Committee on March 5, 2009 (ML090780178)

5. Slides 13 and 15 of the Staff’s Presentation Materials on RG 5.71 Cyber Security Programs for Nuclear Facilities, presented to the Committee on March 5, 2009 (ML090780178)

1. Regulatory Guide RG 5.71, “Cyber Security Programs for Nuclear Facilities,” Nuclear Regulatory Commission, Washington, DC, January 2009 (ML090760860)

2. Letter from William J. Shack, Chairman, ACRS, to Dale E. Klein, Chairman, NRC, Subject: Digital Instrumentation and Control Systems Interim Staff Guidance, dated April 29, 2008 (ML081050636)

3. Draft Regulatory Guide DG-5022, “Cyber Security Programs for Nuclear Facilities,” Nuclear Regulatory Commission, Washington, DC, December 2008 (ML090760900)

4. Slide 8 of the Staff’s Presentation Materials on RG 5.71 Cyber Security Programs for Nuclear Facilities, presented to the Committee on March 5, 2009 (ML090780178)

5. Slides 13 and 15 of the Staff’s Presentation Materials on RG 5.71 Cyber Security Programs for Nuclear Facilities, presented to the Committee on March 5, 2009 (ML090780178)

Distribution:

CSantos	ADias	DBessette
HNourbakhsh	GShukla	MBanerjee
PWen	ZAbdullahi	SDuraiswamy
HVandermolen	CLBrown	DWidmeyer
MLee	JFlack	VBrown
JDelgado	NColeman	CJaegers
TBloomer	BChamp	ABates
C. Antonescu	V. Perin	RidsSECYMailCenter
SMcKelvin	LMike	RidsNSIROD
RidsEDOMailCenter	RidsNMSSOD	RidsOIGMailCenter
RidsFSMEOD	RidsRESOD	RidsOCAAMailCenter
RidsOGCMailCenter	RidsOCAMailCenter	J. Ridgely
RidsNRROD	RidsNROOD	

Accession No: **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
Package: ML090780149
Letter: ML090700457
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	A. Dias for C. Antonescu	A. Dias for C. Antonescu	C. Santos	E. Hackett	E. Hackett for M. Bonaca
DATE	03/19/09	03/19/09	3/19/09	3/19/09	3/19/09

OFFICIAL RECORD COPY