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

November 12, 2009

The Honorable Gregory B. Jaczko
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 Jaczko:

During the 567th meeting of the Advisory Committee on Reactor Safeguards, November 5-7, 2009, we reviewed the November 2009 version of draft final Regulatory Guide (RG) 5.71, “Cyber Security Programs for Nuclear Facilities.” Our Digital Instrumentation and Control Systems Subcommittee also reviewed this matter during a meeting on October 23, 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

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

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.

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

4. Longer-term research projects should be initiated by the Office of Nuclear Regulatory Research 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

BACKGROUND AND DISCUSSION

10 CFR 73.54 requires, in part, that licensees submit a cyber security plan and implementation schedule for NRC review and approval by November 23, 2009. A further requirement is that licensees provide high assurance that digital computer and communication systems and networks associated with safety and security functions are adequately protected against cyber attacks up to and including the design basis threat as described in 10 CFR 73.54. This high

assurance is expected to be accomplished by first identifying these assets, and, second, developing a cyber security program for their protection.

RG 5.71 is intended to provide an approach that the NRC staff finds acceptable for complying with the requirements of this regulation. Such an approach would promote consistency among licensee submittals, reviewer evaluations, and inspector activities; thereby providing effective cyber security.

In developing this Regulatory Guide, the staff has relied heavily on NIST Standards, in particular, NIST SP 800-53, Rev. 3, “Recommended Security Controls for Federal Information Systems,” and NIST SP 800-82, “Guide to Industrial Control Systems Security.”

Short-term Issues

10 CFR 73.54 requires licensees to develop cyber security policies and plans. The rule also requires that digital assets be protected with high assurance. RG 5.71 provides guidance for licensees to develop cyber security policies and plans without providing guidance for the assessment of their adequacy.

Although Appendix A, Section A.2.2, of RG 5.71 is titled “Performance-Based Requirements,” it does not identify performance measures that can be used as convincing indicators of high-assurance that digital assets are protected against cyber attacks. Such indicators might include: (1) degree of critical system data and communication isolation, (2) degree and depth of system configuration management and controls, and (3) degree and level of system access control. The regulatory guide, in essence, assumes that a licensee can ultimately meet the cyber-security protection requirements of the regulation by selecting and implementing a set of security controls from a pre-determined list. These controls are based on generic (i.e., non-nuclear-plant specific) control compilations documented in the NIST Standards. Some flexibility is built into the prescriptive approach by allowing licensees to forgo the use of certain controls if it can be shown that these are not applicable to the specific Critical Digital System (CDS) or Critical Digital Asset (CDA) to be protected.

The staff stated that licensees are already implementing this regulatory guide to support timely compliance with 10 CFR 73.54. The initial applications will provide insights into the usefulness of the guidance in the development of cyber security plans and policies. We recommend that such experience be collected and lessons learned produced so that the regulatory guide can be revised to improve its effectiveness.

Long-term Issues

A plant-specific PRA identifies the accident sequences that may lead to core damage. A successful cyber attack would have to trigger one of these sequences. This recognition would allow the analysts to focus on those digital assets that may affect these sequences and, in particular, the assets whose failure could cause an initiating event and the dependent failures of safety systems appearing in the same sequence. This approach would be analogous to the current evaluations of the risks from fires, earthquakes, and other “external” events. Performing such an analysis would be a significant step toward risk-informing the cyber security guidance.

More guidance is needed regarding the interaction between safety and security. In existing plants, many of the security controls recommended by RG 5.71 will be installed in the communications paths used to control reactor operation. Not only must the security control be analyzed to ensure that it will not interfere with operator response to a safety incident, but the possibility of security control failure (i.e., “locking out” inadvertently) must be an element of the overall safety analysis. A provision for “authorized break-in” or “emergency override” capability in security controls then introduces vulnerabilities in that an attacker may “spoof” operators into invoking this capability.

As identified in the regulatory guide, a potential attack vector is a supply-chain attack, i.e., the deliberate insertion of malicious functionality at any point from vendor facility through distribution and into maintenance (software update) processes. Such attacks are potent weapons against defense-in-depth. Defense against such attacks requires long lead time activities such as the establishment of trusted distribution paths, validation of vendors, procurement or development of tamper-proof or tamper-evident seals, and other steps that must be integrated into the operation of a protected site. Research activities in this area should be started.

The staff is dealing with a very difficult problem for which the state of regulatory practice is in its infancy. Collecting experience from licensee implementation of the regulatory guide and performing long-term research in selected areas is a reasonable way to move forward.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

References

1. NRC: Cyber Security Programs for Nuclear Facilities, 11/2009 (Regulatory Guide 5.71) (ML092670517) Official Use Only – Security-Related Information

2. NIST SP 800-53, Rev. 3, “Recommended Security Controls for Federal Information Systems,” National Institute of Standards and Technology, Gaithersburg, MD, 08/2009

3. NIST SP 800-82, “Draft Guide to Industrial Control Systems (ICS Security),” National Institute of Standards and Technology, Gaithersburg, MD, 09/2008

More guidance is needed regarding the interaction between safety and security. In existing plants, many of the security controls recommended by RG 5.71 will be installed in the communications paths used to control reactor operation. Not only must the security control be analyzed to ensure that it will not interfere with operator response to a safety incident, but the possibility of security control failure (i.e., "locking out" inadvertently) must be an element of the overall safety analysis. A provision for "authorized break-in" or "emergency override" capability in security controls then introduces vulnerabilities in that an attacker may "spoof" operators into invoking this capability.

As identified in the regulatory guide, a potential attack vector is a supply-chain attack, i.e., the deliberate insertion of malicious functionality at any point from vendor facility through distribution and into maintenance (software update) processes. Such attacks are potent weapons against defense-in-depth. Defense against such attacks requires long lead time activities such as the establishment of trusted distribution paths, validation of vendors, procurement or development of tamper-proof or tamper-evident seals, and other steps that must be integrated into the operation of a protected site. Research activities in this area should be started.

The staff is dealing with a very difficult problem for which the state of regulatory practice is in its infancy. Collecting experience from licensee implementation of the regulatory guide and performing long-term research in selected areas is a reasonable way to move forward.

Sincerely,
/RA/
Mario V. Bonaca
Chairman

Distribution:
See next page

Accession No: ML093130111 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	ADias/CSantos	EHackett	MBonaca
DATE	11/ 12 /09	11/ 12 /09	11/ 12 /09	11/ 12 /09	11/ 12 /09

OFFICIAL RECORD COPY

Letter to the Honorable Gregory B Jaczko, Chairman, NRC, from Mario V. Bonaca, Chairman, ACRS, dated November 12, 2009

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

Distribution:
ACRS Branch A
ACRS Branch B
E. Hackett
H. Nourbakhsh
J. Flack
C. Jaegers
T. Bloomer
B. Champ
A. Bates
S. McKelvin
L. Mike
J. Ridgely
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter