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

December 16, 2021

Mr. Daniel H. Dorman
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: PROPOSED DRAFT REGULATORY GUIDE 5.71, REVISION 1, "CYBER SECURITY PROGRAMS FOR NUCLEAR POWER REACTORS"

Dear Mr. Dorman:

During the 691st meeting of the Advisory Committee on Reactor Safeguards, November 30 through December 3, 2021, we reviewed "Proposed Draft Regulatory Guide (RG) 5.71 (Draft Guide 5061, Revision 1), Revision 1, 'Cyber Security Programs for Nuclear Power Reactors,' Draft Issued: July 2021." Our Digital Instrumentation and Control (DI&C) Systems Subcommittee also reviewed this matter on October 22, 2021. Prior to this review, we had the benefit of discussions with representatives of the NRC staff during a DI&C Systems Subcommittee meeting on an Overview of DI&C Regulatory Activities on September 22, 2021. We also had the benefit of the documents referenced.

CONCLUSIONS AND RECOMMENDATIONS

1. The efforts by the staff to revise the application of RG 5.71 over the last 10 years were important, timely, and fruitful. The original guidance was revised to be more clear in its application and less cumbersome to maintain and monitor the critical area of cyber protection.

2. Reactor safety, engineered safeguards, reactor and plant controls, monitoring and many balance-of-plant (BOP) systems cannot have malware detection and mitigation software incorporated into their digital/computer-based operating system software without impairing functionality. To ensure that the new electronic access pathways introduced by digital data transmission are not compromised, DI&C license amendment request (LAR) upgrades and new reactor design applications must rely on DI&C architecture designs that incorporate uni-directional, hardware based, not configured by software devices (i.e., data diodes) where needed.

3. We recommend several changes for incorporation into proposed draft RG 5.71, Revision 1, to provide context and improve clarity prior to issuing for public comment.

BACKGROUND

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54 requires that licensees have a cyber security plan and implementation schedule for NRC review. 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 identifying their assets and 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.

This proposed Revision 1 to RG 5.71 incorporates lessons learned from operating experience since original publication of the guide in January 2010. Specifically, this revision clarifies issues identified from cyber security milestone inspections, additional insights gained through the Security Frequently Asked Questions process, documented cyber security attacks, new technologies, and new regulations. Also, this revision considers the changes in the most recent revision to National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, September 2020, and updates reference to RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3.

DISCUSSION

The staff organizes, in RG 5.71, a broad range of issues that must be addressed in any cyber security program for nuclear power plants. They begin by identifying an extensive list of the elements of a cyber security plan. The heart of the guidance is Section C.3 on establishing and implementing the program. They proceed to explain how to analyze digital systems to identify critical digital assets, including a process to limit the extent of this work by focusing on the more important assets. As they begin the discussion of how to protect those assets, we find that they miss an opportunity to identify what is unique about digital systems compared to the earlier analog systems. For most attack pathways, such as attacks on the supply chain, portable media and mobile devices, wireless equipment, and physical presence pathways, the protection strategies are the same for both types of systems. However, digital systems, despite their many advantages, open up a new attack pathway: some entity outside (or inside) the facility that use digital signals to attack the assets. Here, the most reliable mechanism to interfere with the ability to send signals into the systems and networks is the use of uni-directional hardware-based data communications mechanisms (not implemented in software), typically called a data diode. The data diode and physical access control each provide protection for the attack pathway the other cannot provide. It is also important to protect against bypass of the data diode function for any reason, by including defense-in-depth options.

The guidance goes on to describe security controls to prevent attacks including technical, operational, and management security controls. To support the important area of technical control of access, the staff provides Appendix B with many details and examples to support users of the guidance. However, we continue to be concerned about electronic control of access for internal DI&C systems or for communication from in-plant to external systems and in-plant systems to in-plant systems both across and within the same defensive level. RG 5.71 should explicitly recognize that reactor safety, engineered safeguards, reactor and plant controls, monitoring and many BOP systems cannot have malware detection and mitigation software incorporated into their digital/computer-based operating system software without impairing functionality. To ensure that the new electronic access pathways introduced for digital data transmission cannot be compromised, these systems must rely on incorporating data

diodes in the overall DI&C architecture design during the design phases of both DI&C LAR upgrades and new reactor design applications for situations where there are communications between high safety-significance systems and those of lower safety-significance both across and within defensive security levels.

Data diodes prevent either remote (internet susceptible) introduction of malware or its propagation from lower safety significance to higher safety significance systems, if not detected by access controls (e.g., the administrative personnel physical presence pathways/access to the equipment and supply chain controls system detection processes).

Our concern is time-sensitive given potential applications related to DI&C systems for new designs and upgrade replacements. The staff does not have any plans, in the near future, to revise the guidance documents used during design reviews for any operating plant upgrades or new plant design application reviews. Waiting until cyber reviews are performed is too late. RG 5.71 is the only document currently under revision that could clarify that only data diodes should be used when there are communications between high safety-significance systems and those of lower safety-significance both across and within defensive security levels. This is important during design reviews before a cyber security program has been established.

Proposed Changes

Section A - Applicability – We recommend that this section be clarified to expand the applicability of RG 5.71 as a resource for design reviews. At that time the overall system architectures are being developed during the licensing design certification phase by new applicants, and for LARs for operating plant upgrades, even if a cyber security program review has not been established.

Section C.3.2 - We recommend that this section be revised to explain that safety and safety-related systems, and many BOP systems cannot have malware detection and mitigation software incorporated into their digital/computer-based operating system software, since it could impair their ability to perform their safety and plant control functions. It should then state that data diodes for preventing electronic access in concert with physical control of access to systems are complementary in that they each protect a pathway that the other cannot.

Section C.3.2.1, Paragraph 2 – Sentence 3 – We recommend that this sentence be clarified to include evaluations between high safety significance to lower safety significance systems within a security level. Data communications between systems within a security level are just as critical.

Glossary – Data diode should be added to the glossary and defined as a uni-directional, hardware-based, not configured by software data transmission device. In addition, the term one-way should be added and defined as synonymous with data diode for clarity and consistency.

Summary

The efforts by the staff to revise the application of RG 5.71 over the last 10 years were important, timely, and fruitful. The revisions improve the original guidance to be more clear in its application and less cumbersome to maintain and monitor the critical area of cyber protection.

We continue to be concerned with electronic control of access. Because malware detection and mitigation software impair safety and plant control systems functionality, a data diode is the most reliable means to prevent external access to digital systems. Therefore, the use of data diodes should be considered during the design phase.

Also, we recommend several changes for incorporation into proposed Revision 1 to RG 5.71 to provide context and improve clarity prior to issuing for public comment.

We look forward to working with the staff as they finalize this regulatory guide.

Sincerely,

Signed by Sunseri, Matthew on 12/16/21

Matthew W. Sunseri
Chairman

REFERENCES

1. Regulatory Guide (RG) 5.71, “Cyber Security Programs for Nuclear Facilities,” Revision 1, July 2021 (ML21095A329)

2. Regulatory Guide (RG) 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Revision 3, July 3, 2011 (ML102870022)

3. U.S. Nuclear Regulatory Commission, “Review of NUREG-0800, Branch Technical Position 7-19, ‘Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure due to Latent Design Defects in Digital Safety Systems,’ Revision 8,” December 18, 2020 (ML20345A338)

4. National Institute of Standards and Technology (NIST), NIST SP 800-53, “Security and Privacy Controls for Information Systems and Organizations,” Revision 5, September 2020.

5. Advisory Committee on Reactor Safeguards, “Uni-Directional Communications (Not Implemented in Software) from High Safety to Lower Safety Systems and Internal Plant to External Systems Connected to the Internet,” March 31, 2020 (ML20328A157)

6. U.S. Nuclear Regulatory Commission, “The Advisory Committee on Reactor Safeguards Memorandum titled: Uni-Directional Communications (Not Implemented in Software) from High Safety to Lower Safety Systems and Internal Plant to External Systems Connected to the Internet,” April 14, 2021 (ML21112A190)

7. Office of Nuclear Security and Incident Response, “Concerns Pertaining to Uni-Directional Communications (Not Implemented in Software) from High Safety to Lower Safety Systems and Internal Plant to External Systems connected to the Internet,” June 30, 2021 (ML21175A332)

8. Executive Director for Operations, “Concerns Pertaining to Uni-Directional Communications (Not Implemented in Software) from High Safety to Lower Safety Systems and Internal Plant to External Systems Connected to the Internet,” July 14, 2021 (ML21187A293)

December 16, 2021

SUBJECT: PROPOSED DRAFT REGULATORY GUIDE 5.71, REVISION 1, "CYBER SECURITY PROGRAMS FOR NUCLEAR POWER REACTORS"

Accession No: ML21342A263 **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	LBurkhart	SMoore	MSunseri
DATE	12/9/21	12/9/21	12/9/21	12/16/21	12/16/21

OFFICIAL RECORD COPY