UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 28, 2022

Dr. Joy L. Rempe, Chairman
Advisory Committee on Reactor Safeguards
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 Dr. Rempe:

The purpose of this letter is to provide the U.S. Nuclear Regulatory Commission (NRC) staff's response to the Advisory Committee on Reactor Safeguards (ACRS or the Committee) letter dated December 16, 2021 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML21342A263), on "Proposed Draft Regulatory Guide (RG) 5.71 (Draft Guide [DG] 5061), Revision 1, 'Cyber Security Programs for Nuclear Power Reactors', Draft Issued: July 2021."

During the 691st meeting of the ACRS that took place November 30–December 2, 2021, the ACRS reviewed the DG 5061. Previously, the ACRS Digital Instrumentation and Control (DI&C) Subcommittee reviewed this topic on October 22, 2021. In the letter dated December 16, 2021, the ACRS provided conclusions and recommendations along with four proposed changes to DG 5061. The NRC staff appreciates the ACRS feedback and has made corresponding changes to DG 5061, which will be incorporated into the version to be released for public comment. Specific NRC staff responses to the ACRS proposed changes follow.

Proposed ACRS Change 1:

> *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 [licensing amendment requests] for operating plant upgrades, even if a cyber security program review has not been established.*

NRC Staff Response 1:

The NRC staff agrees with the Committee's suggestion to specify that this guidance may be used by applicants and licensees during design development activities. The staff made the following change to Section A "Applicability" in DG 5061 (new text is underlined):

> This RG applies to operating power reactors licensed in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." This RG may also be

used as a resource by power reactor applicants and licensees during design development of digital safety systems.

Proposed ACRS Change 2:

Section C.3.2 - We recommend that this section be revised to explain that safety and safety-related systems, and many BOP [balance-of-plant] 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.

NRC Staff Response 2:

The NRC staff agrees that some safety, safety-related, and BOP systems cannot have malware detection and mitigation software incorporated into their software and/or firmware, since it could impact safety functions. Furthermore, data diodes prevent electronic access in concert with physical control of access to systems, each protecting a pathway that the other cannot. The staff has chosen the wording of Section C.3.2 "Defense-in-Depth Protective Strategies" to be consistent with the regulatory requirements for defense-in-depth and reinforce the importance of protections that work in concert to provide both complementary and redundant security controls:

> From a defensive architecture perspective, defense-in-depth involves setting up multiple security boundaries to protect CDAs [critical digital assets] and networks from a cyber attack…. Defense-in-depth defensive strategies are represented by documented collections of complementary and redundant security controls that establish multiple layers of protection to safeguard CDAs. Under a defense-in-depth defensive strategy, the failure of a single protective strategy or security control should not result in the compromise of a safety, important-to-safety, security, or emergency preparedness function.

The application of specific controls, such as malware detection and mitigation software, is addressed in Section C.3.3 "Security Controls." The NRC staff agrees with the Committee that cyber protections should not impair the ability to perform safety and plant control functions. The specific guidance in Section C.3.3. states:

> A security control should not be applied if the control adversely impacts SSEP [safety, important-to-safety, security, or emergency preparedness] functions or performance (e.g., unacceptable change in system response time, undesirable increase in system complexity). When a security control is determined to have an adverse effect, the licensee should use alternate controls to protect the CDA from a cyber attack….

Proposed ACRS Change 3:

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.

NRC Staff Response 3:

The NRC staff agrees with the Committee and made the recommended change to Section C.3.2.1 in DG 5061 (new text is underlined):

> While the defense architecture may allow communications between systems within the same level (e.g., Level 4 or Level 3), the digital isolation of critical digital assets (CDAs) (i.e., no digital communication pathways between a CDA and any other digital asset) is a mechanism to meet many of the requirements specified in 10 CFR 73.54. Incorporating analog communication at strategic points within the defensive architecture is one example of digital isolation implementation. Data communication between systems within the same security levels should be protected commensurate with the security and safety significance of the communicating critical systems (CSs) or CDAs.

Proposed ACRS Change 4:

> *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.*

NRC Staff Response 4:

The NRC staff agrees with the Committee and has added the term Data Diode to the glossary. The staff consulted NIST SP 800-82[1] revision 2, which gives the following definition: “A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction.” The staff has tailored the NIST definition for data diode to incorporate the Committee’s recommendation to specify that the data diode is hardware-based and affirm that

[1] National Institute of Standards and Technology Special Publication 800-82, “Guide to Industrial Control Systems (ICS) Security,” Revision 2, May 2015

communications must be physically unable to flow in more than one direction. The following definition for data diode will be added to the glossary section of DG 5061:

> Data Diode – a hardware device that permits data to flow from one network to another but is physically unable to send any information at all back into the source network.

The staff appreciates your review of DG 5061 and looks forward to future interactions with the ACRS.

Sincerely,

Signed by Gavrilas, Mirela
on 01/28/22

Mirela Gavrilas, Director
Office of Nuclear Security and
Incident Response

cc: OCM
SECY

ACRS Letter - Proposed Draft Regulatory Guide 5.71, Revision 1, Cyber Security Programs ForNuclear Power Reactors - Staff Response DATE January 28, 2022

DISTRIBUTION: OEDO-21-00538
MGavrilas, NSIR
MSampson, NSIR/DPCP/RSB
ELee, NSIR/DPCP/CSB
EBenner, NRR/DEX
CRaynor, NSIR/PMDA
SHoliday, NSIR/DPR
SRodriguez, OEDO
RidsACRS_MailCTRResource, ACRS
RidsEdoMailCenterResource, OEDO
RidsNrrDex, NRR/DEX
JBeardsley, NSIR/DPCP/CSB
JJohnston, NRR/DEX/EICA
RidsNsirMailCenterResource, NSIR

ADAMS Accession No.: Ltr ML22014A419 *** via email**

OFFICE	NSIR/DPCP/CSB	NSIR/DPCP/CSB	NSIR/DPCP/RSB*	NRR/DEX
NAME	KLawson-Jenkins *KL*	ELee *EL*	MSampson *MS*	EBenner *EB*
DATE	Jan 17, 2022	Jan 18, 2022	Jan 18, 2022	Jan 18, 2022
OFFICE	NSIR/PMDA	NSIR		
NAME	CRaynor *CR*	MGavrilas *MG*		
DATE	Jan 27, 2022	Jan 28, 2022		

OFFICIAL RECORD COPY