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

June 30, 2021

MEMORANDUM TO: Andrea D. Veil, Director
Office of Nuclear Reactor Regulation

Mirela Gavrilas, Director
Office of Nuclear Security and Incident Response

FROM: Michele M. Sampson, Deputy Director *Michele Sampson*
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

SUBJECT: 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

This memorandum summarizes the results of our independent review of information provided in the March 31, 2021, letter from Mathew W. Sunseri, Chairman of the Advisory Committee on Reactor Safeguards (ACRS), to Chairman Hanson, 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" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML21085A014).

The Chairman's April 14, 2021, memorandum (ADAMS Accession No. ML21112A190) directed the Executive Director for Operations to undertake a review to provide the Commission information on how the concerns raised by the ACRS have been addressed. In response to the Chairman's memorandum, Margie Doane, Executive Director for Operations, requested that you assemble an independent team of experts (Team) to respond to the matters raised in the ACRS' letter. Team members include: Billy Dickson, Region III; James Maltese, Office of the General Counsel; Erick Martinez Rodriguez, Office of Nuclear Regulatory Research; Johari Moore, Office of Nuclear Security and Incident Response (NSIR); MJ Ross-Lee, Office of Nuclear Reactor Regulation (NRR); and Michele Sampson, NSIR.

The Team reviewed the concerns raised by the ACRS, specifically, that the use of a uni-directional hardware device should be required at the nuclear power reactor design phase. The Team conducted a peer review of how the concerns raised by the ACRS were addressed by the staff and evaluated whether additional regulatory actions are warranted. As part of this task, the Team conducted interviews with technical staff from NRR and NSIR and held an

CONTACT: Michele Sampson, Team Lead
301-415-7493

information-gathering meeting with ACRS member Charles Brown to seek clarification on the concerns raised by the ACRS. The Team used the Be riskSMART framework to consider the challenges and opportunities associated with potential regulatory action to address the concerns.

BACKGROUND

Concerns Raised by the ACRS

In its March 31, 2021, letter to the Chairman, the ACRS stated that "Commission direction is needed for the staff to assure, during design reviews, that only uni-directional hardware-based data communications mechanisms (not implemented in software) are used when there are communications between High Safety-Significance systems and those of Lower Safety-Significance." The ACRS stated that such hardware is the way to safeguard digital instrumentation and control (DI&C) systems from compromise.

ACRS noted that Section B.2.2. of the November 2019 version of the draft Branch Technical Position (BTP) 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 (ADAMS Accession No. ML20339A647), included language that, in ACRS' view, "emphasized that interconnections between High Safety-Significance systems and those of Lower Safety-Significance should be accomplished through the use of one-way digital communication devices rather than bi-directional communication devices," but that the staff removed this language from subsequent versions. ACRS pointed to its November 23, 2020, letter to the staff (ADAMS Accession No. ML20328A157) recommending that the BTP "be revised to ensure that interconnections between High Safety-Significance systems and those of Lower Safety-Significance are one-way, uni-directional (not implemented in software) digital communication devices."

ACRS also stated that the staff's current approach of addressing cyber security for DI&C digital data communications architecture during the operating license application review is "too late," and recommended that Regulatory Guide (RG) 5.71, "Cyber Security Program for Nuclear Facilities" (ADAMS Accession No. ML090340159), be used during the design certification phase of an application. ACRS indicated that the guidance "would have licensees place all digital safety systems in the highest level of their defensive architecture and only permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture."

Branch Technical Position 7-19

BTP 7-19 provides the U.S. Nuclear Regulatory Commission (NRC) staff with guidance for evaluating an applicant's assessment of defense-in-depth and diversity (D3) adequacy for a proposed DI&C system. This document is part of the suite of guidance in the "Standard Review Plan [SRP] for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (NUREG-0800). The SRP establishes criteria that the NRC staff uses in evaluating whether an application meets the NRC's regulations. The SRP is not a substitute for the NRC's regulations and compliance with it is not required.

In November 2019, the staff provided a draft of Revision 8 to BTP 7-19 to the ACRS for review. Section B.2.2. of this draft provided guidance to the staff on assessing common-cause failures. The draft guidance included an example of how the staff's D3 review could be tailored based on whether the design included uni-directional digital communications between safety systems of higher and lower safety significance.[1] This example was not intended to emphasize that applicants should use one-way communication hardware in their design, but it was instead intended to assist the staff in identifying a mechanism that could be used by an applicant to exclude lower safety significant systems from being considered in the D3 assessment. During the Team's discussions with the staff regarding this example, the staff explained that the example was likely removed from the document as an administrative edit and the staff did not object to the example or its reinsertion.

Regulatory Guide 5.71

RG 5.71 provides guidance to applicants that describes an acceptable approach for complying with the NRC's regulations in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and networks." The framework included in the guidance describes a defensive architecture that establishes formal communication boundaries and defensive measures against cyber attacks. Within the framework, communications from digital assets at higher security levels would be one-way to the lower security levels, such as site administrative networks and the internet. The use of uni-directional communications hardware is described as an acceptable means to implement this one-way communications control. To demonstrate compliance with the cyber security requirements, licensees must implement defense-in-depth strategies (a documented collection of complementary and redundant security controls that establish multiple layers of protection) and account for the site-specific conditions that affect implementation. Licensees may use methods other than those described within RG 5.71 to meet the NRC's regulations if the chosen measures satisfy the stated regulatory requirements.

DISCUSSION

The Team evaluated the concerns articulated by the ACRS to determine whether a new safety or security issue that is not covered by the NRC's regulations for current licensees or future applicants was identified. Furthermore, the Team considered the actions taken by the staff prior to publication of BTP 7-19 and the additional actions identified within the ACRS letter. The Be riskSMART framework was used as a systematic approach by the Team to make risk-informed recommendations to address the concerns.

[1] The draft guidance stated: "If the licensee or applicant can demonstrate that existing or newly created interfaces or interconnections between A1 systems and systems in other categories do not have the potential to adversely impact the operation of the A1 systems (e.g., use of one-way digital communications output from the A1 system to systems in other categories rather than bi-directional communications) or reduce defense-in-depth, then the impacts of failures occurring within the non-A1 system(s) can be excluded from the D3 assessment for the A1 system."

Under the current regulations in 10 CFR 73.54, all operating nuclear power reactor licensees are required to implement cyber security protections for digital communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions. For operating license or combined license (COL) applicants, the staff reviews an applicant's cyber security plan before issuing the license to verify that the applicant's proposed cyber security protections (which may include a uni-directional hardware device as one element) will provide the requisite assurance that SSEP functions will be protected from cyber attacks.

The Team examined the current practices of the operating nuclear power reactor fleet to assess how the ACRS concerns regarding two-way communications are addressed. The use of hardware to separate the SSEP functions from external and business system networks, like a virtual "security fence" around them, is a proven approach for the existing fleet where all of these functions are physically housed at the operating nuclear power reactor site. All current operating nuclear power reactors have committed to a uni-directional communication hardware device to separate the protected networks from any external networks as part of their cyber security programs.

However, the Team identified that the virtual "security fence" approach and its reliance on uni-directional communications hardware may not be easily applicable or effective for advanced nuclear power reactor designs contemplating innovative approaches such as remote or autonomous operations. Mandating this hardware in the NRC's regulations would add a prescriptive requirement to the current performance-based regulations that could result in the need for future exemptions.

The current regulatory framework applies cyber security requirements at the time of an operating license or COL application. The NRC's cyber security requirements are performance based, and while some aspects could be reviewed during the design certification review, such as protections for the safety functions, other elements like protections for physical security and emergency preparedness functions would not be expected to be sufficiently complete for the staff to review until the operating license or COL application is submitted. To effect the ACRS recommendation to review cyber security at the design certification application phase, regulatory change would be needed. The more fulsome review and approval of the cyber security plan, which includes consideration of physical security and siting, would still occur during the operating license or COL application review. The addition of an NRC review of cyber security during the design certification review phase would add a burden to applicants and potentially increase the cost of the design review without increasing security, since the requirement for full compliance with 10 CFR 73.54 still applies to the operating nuclear power reactor facility.

Noting the cyber events identified in the ACRS letter, the Team considered the evolving nature of the cyber threat. The underlying cyber risk is periodically reassessed through the NRC's threat assessment process. This process considers cyber incidents at other facilities, including, for example, the Colonial Pipeline attack and other recent events identified in the ACRS letter. This periodic assessment serves to verify that the NRC's cyber security requirements are adequate to protect SSEP functions at operating nuclear power reactors.

Staff from NRR and NSIR have documented roles and responsibilities to work together during licensing reviews. During licensing reviews, NRR staff reviews the safety aspects of an

application while NSIR staff evaluates the adequacy of cyber security features for compliance with 10 CFR 73.54. The NRR staff communicates with NSIR if any cyber security concerns or design features are identified during the review of the DI&C systems to ensure that any cyber security design features included as part of a safety-related system to comply with 10 CFR 73.54 do not adversely affect the reliable performance of the safety function of the DI&C system.

The ACRS identified that a potential impact of performing the cyber security review after completing the design review is delay or additional cost to the applicant during the operating license or COL application review. The Team considered the guidance documents identified by the ACRS and Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML102870022), and evaluated whether additional information could be included to address this ACRS concern by raising awareness of the cyber security requirements for design certification applicants.

CONCLUSION

The Team concluded that the concerns identified by the ACRS' letter do not identify a safety issue not currently covered by the NRC's regulations (i.e., no regulatory gap exists that could lead to a safety or security issue) for existing licensees or future applicants. Mandating hardware would not increase the level of cyber security protection. It would add a regulatory burden, reduce flexibility, and make the NRC's regulations more prescriptive in an area where performance-based regulations have proven effective. The Team further concluded that specific guidance documents could be revised to encourage design certification applicants to consider the cyber security requirements that will apply to a future operating license or COL applicant.

RECOMMENDATIONS

The Team recommends that during the next revision of BTP 7-19 the staff include language, consistent with the example that the staff previously removed, that clarifies how the staff could reduce the scope of its review of the D3 assessment when a design includes uni-directional digital communications between safety system tiers. The recommended revision would serve to raise awareness of this option for the staff and applicants. Applicants whose designs do not include this feature would be subject to the portion of the staff's review of the D3 assessment that considers the hazards of bi-directional digital communications across safety system tiers.

The Team recommends that the staff revise RG 1.152 to reference RG 5.71 and include additional information to make applicants for design certifications aware of the cyber security requirements that apply to an operating license or COL, and how these requirements could be considered during the design phase.

The Team recommends that the staff revise RG 5.71 to reference RG 1.152 to make applicants for design certification aware of cyber security controls that could be incorporated as part of the nuclear power reactor design.

SUBJECT: 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

DATED: June 30, 2021

DISTRIBUTION:

M. Doane OEDO
D. Dorman, OEDO
C. Haney, OEDO
RidsNrrOd
RidsNsirOd
RidsResOd
Ridsrgn3MailCenter Resource
RidsOgcMailCenter Resource

Ticket SRM-CTH210414-1
ADAMS Accession Number: ML21175A332 ***via email**

OFFICE	NSIR/DPCP	NSIR/DPCP	NRR/DSS	RES/
NAME	M Sampson	J Moore	MJ Ross-Lee	E Martinez
DATE	06/30/21	06/30/21	06/30/21	06/30/21
OFFICE	RIII	OGC	NRC/NSIR/Tech ed	
NAME	B Dickson	J Maltese	C Raynor	
DATE	06/30/21	06/30/21	06/30/2021	

OFFICIAL RECORD COPY