PUBLIC SUBMISSION

SUNI Review Complete
Template=ADM-013
E-RIDS=ADM-03

ADD: Bridget Curran, Mekonen Bayssie, Mary Neely
Comment (4)
Publication Date: 3/3/2022
Citation: 87 FR 12208

As of: 5/4/22 9:57 AM
Received: May 02, 2022
Status: Pending_Post
Tracking No. l2p-66v6-r2ql
Comments Due: May 02, 2022
Submission Type: Web

Docket: NRC-2021-0143
Cyber Security Programs for Nuclear Power Reactors

Comment On: NRC-2021-0143-0001
Cyber Security Programs for Nuclear Power Reactors

Document: NRC-2021-0143-DRAFT-0006
Comment on FR Doc # 2022-04464

Submitter Information

Email: alowry@ameren.com
Organization: Ameren - Callaway Energy Center

General Comment

See attached file(s)

Attachments

Comments for DG-5061 Rev 1

Comments for DG-5061, Rev 1, Cyber Security Programs for Nuclear Power Reactors

General – document layout

It is confusing that section C of the Reg Guide body and Appendix C both have sections numbers that start with C. Then, in the template in Appendix A, the C is dropped when referring to guidance from section C of the Reg Guide body. Suggest eliminating the C from the section numbers in the Reg Guide body.

The first part of the Appendix A template basically requires doing everything in section 3.3 of the main Reg Guide section C. Following template sections sometimes repeat the language from the Reg Guide body and sometimes refer back to other sections of the body. This makes it difficult to read through the resulting Cyber Security Plan and determine what is being done. It would be necessary to always keep a copy of the Reg Guide in hand in order to determine what is required by the Cyber Security Plan if the template is used. Suggest incorporating the Reg Guide language into the Appendix A template so that a stand-alone Cyber Security Plan document is created from the template.

Glossary

Critical digital Asset (CDA) – This definition is incomplete and would result in any digital device in a critical system being considered a CDA. When systems are evaluated, all system functions are examined and if ANY of these are SSEP functions, then the system is classified as a critical system. There could be stand-alone digital devices in this system, however, that only perform non-SSEP functions. These devices would not be classified as CDAs, even though they are digital components in a critical system. The definition needs to include bounding criteria regarding the digital device performing / supporting / protecting a SSEP function.

Attack vector and attack pathway – These definitions do not align with the industry use of these terms. While the term threat / attack vector is used extensively throughout several NRC approved NEI documents, the only place this term has been defined is in NEI 10-09. While this document was not approved by the NRC and is generally not used by the industry, the industry has adopted its terminology for pathways and attack vectors as these were not defined elsewhere. This document states:

For the purposes of implementing cyber security plans, pathways that introduce vulnerabilities are associated with the following attack vectors:

1) Direct Network Connectivity

2) Wireless Network Capability

3) Portable Media and Equipment

4) Supply Chain

5) Direct Physical Access

Licensees have developed their justifications for addressing security controls using this definition. Per NEI 08-09 section 3.1.6 (and Reg Guide A.3.1.6), not implementing a security control may be justified by demonstrating the attack vector does not exist. The industry understanding is that these justifications are based on evaluating the pathway rather than the method and while the results may typically be the

same, this could be considered a change in philosophy. The best solution could be to move away from the attack vector term and simply focus on evaluating the threat the security control protects against and determining whether that threat exists for the specific CDA. This could then be addressed by eliminating either the method or the pathway. In any case, this is an item that needs to be addressed. If the NRC position is that the industry needs to be specifically evaluating the attack mechanism and not the pathway, then this is a change in philosophy that needs to be communicated. If the intent is just to evaluate the threat and it is acceptable to justify that the threat does not exist by elimination of either the pathway or method, then section A.3.1.6 (and the NEI documents) should be revised accordingly. To add further confusion, the second paragraph on page 21 indicates that an attack vector is a delivery mechanism or vulnerability/exploit. The attack vector definition, on the other hand, only says it is the mechanism and can be used to exploit a vulnerability.

Specific Section Comments

Page 22

Under the information to collect when following the CDA identification process, clarification is needed to explain what is meant by "developmental and evaluation-related assurance requirements".

Page 28, A-6

The language for implementing alternative controls when a security control cannot be implemented does not align with A.3.1.6, which uses more recently agreed upon language also reflected in NEI 08-09 Addendum 1.

A new bullet was added which states " Apply the security controls described in Appendices B and C to this guide, based on the maximum consequences of a successful cyber attack on the CDAs in terms of plant safety and security". This terminology is vague and does not seem to align with the methodology used for protecting safety and security functions.

Page 37, A-8

The final bullet under integrating the cyber security program into the physical security program discusses periodically exercising the entire security force using multiple realistic scenarios combining both physical and cyber simulated attacks. This requirement would better fit in a physical security Reg Guide as the cyber security organization does not have control over exercising the entire security force. Additionally, in physical security drills, it makes more sense to simulate a cyber attack simply as a failed or compromised piece of equipment that should be assumed to be lost. Cyber security incident response drills and physical attack drills typically follow different timelines and use different response teams, making integration into a single drill impractical. Response to a cyber attack would be integrated with physical security as they are a member of the CSIRT. However, in a physical attack, security would simply be dealing with lost equipment and their response would likely not be impacted by the relatively longer timeline of the CSIRT determining the cause of a cyber attack and recovering a system. The NRC is currently soliciting input regarding integration of cyber security into Force On Force drills, and this is a more appropriate way to drive this particular item.

Page 40

In the first paragraph, clarification is needed regarding the meaning of " This effectiveness analysis should provide key information about the results of previous policy and acquisition decisions".

Page A-2

Under A.3, the reference to 10 CFR 73 Appendix G seems unnecessary as the cyber event reporting was placed in 10 CFR 73.71. Any cyber event causing one of the criteria in Appendix G to be met would also be included as a reportable event in 10 CFR 73.71.

Page A-9

Section A.4.1.1 could be interpreted to require the verification of every security control on every CDA every year. This would be a time consuming and resource intensive effort that would provide little benefit. Discussions with the NRC determined this was not the intent and this was meant more as a review of the effectiveness of the program based controls and to ensure ongoing monitoring of CDAs was occurring. This section should be re-worded to clarify the intent, or possibly be treated as an introduction section for the following sections or integrated into section A.4.1.2.

Page A-10

In the second paragraph of A.4.2, clarification is needed to explain the intent of "address safety, reliability, and security engineering activities".

Appendices B and C

The addition of the "Control Intent" sections provide useful information regarding the threat the control is intended to protect against which then aids in the development of appropriate alternate controls.