Addendum 7 to NEI 08-09, Revision 6 Dated April 2010 Evaluating and Documenting Use of Alternative

Cyber Security Controls / Countermeasures

1 INTRODUCTION

1. BACKGROUND

Nuclear licensees are required in accordance with Appendix A, Section 3.1.6 of their Cyber Security Plans (CSP) to implement cyber security controls in CSP Appendices D and E for CDAs. Where a licensee elects to implement alternative controls/countermeasures, CSP Appendix A, Section 3.1.6.2 establishes the requirements for evaluating and documenting the basis for the use of the alternative controls/countermeasure. During the initial 2017–2018 NRC inspections of the full implementation of the Cyber Security Plan (CSP), Licensees' Critical Digital Asset (CDA) assessment inadequately documented some justifications for the use of alternative cyber security controls/countermeasures under CSP Appendix A, Section 3.1.6.2 for some CDAs. In these cases, the documented basis for applying the alternative controls/countermeasures did not provide for an independent reviewer to conclude that the alternatives mitigated the threat/attack vector the original control was intended to protect. This lack of detail complicated the ability of the NRC inspectors to determine if the applied cyber security controls failed to adequately protect the CDA from a cyber attack or if the issue was only inadequate documentation of the basis for the use of alternative controls/countermeasures.

2. PURPOSE

This addendum documents the process and considerations associated with evaluating and documenting the use of alternative cyber security controls/countermeasures to meet the requirements of CSP Appendix A, Section 3.1.6.2. This addendum intends to enhance clarity and consistency in nuclear licensee implementation of alternative control/countermeasure activities and support NRC oversight activities.

3. SCOPE

The guidance in this addendum is applicable to nuclear power reactor licensees with CSPs based on the template in NEI 08-09, Revision 6, and NEI 08-09, Revision 6, Addendum 1. The guidance in this Addendum is applicable to assessment activities associated with CDAs performed under CSP Appendix A, Section 3.1.6. This guidance may be used by licensees who have used Regulatory Guide (RG) 5.71,"Cyber Security Programs for Nuclear Facilities," as a basis for their Cyber Security Plans. NEI 08-09, Revision 6, Appendix A, Section 3.1.6 corresponds to NRC RG 5.71, Section C.3.3 and Appendix A, Section A.3.1.6.

Section 2 describes the Regulatory Basis for the use of alternative controls/countermeasures associated with assessments performed for CDAs. Section 3 describes an acceptable method for evaluating and documenting the basis for the use of alternative controls/countermeasures to comply with CSP Appendix A, Section 3.1.6.2.

4. USE OF THIS DOCUMENT

This document is intended to be a guide that details an acceptable approach for evaluating and documenting the use of alternative controls/countermeasures for CDAs to comply with CSP Appendix A, Section 3.1.6.2.

5. ACRONYMS

The following acronyms are used in this document:

CDA – Critical Digital Asset

CS – Critical System

CSP – Cyber Security Plan

HMI – Human Machine Interface

RG – Regulatory Guide

SDP – Significance Determination Process

6. DEFINITIONS

None

2 REGULATORY BASIS FOR USE OF ALTERNATIVE CONTROLS/COUNTERMEASURES

The NRC Inspection Procedure for Cyber Security (Reference 5), Section 71130.10-2 provides a discussion on licensee's use of alternative controls that is consistent with the revised text in NEI 8-9 , Revision 6, CSP Appendix A, Section 3.1.6.2. An excerpt of this NRC Inspection Procedure section is restated below:

> "Licensee may elect to implement the controls as specified, implement an alternative, or not implement. For situations in which an alternative control or security measure is provided as a substitute, the licensee shall provide a documented basis that confirms the alternative control mitigates the threat/attack vector the original control is intended to protect and ensures that the functions of protected assets identified by 10 CFR 73.54(b)(1) are not adversely impacted due to cyber attacks. (NEI (A.3.1.6) RG (A3.1.6))
>
> For situations in which the licensee has determined the control is unnecessary (e.g., the threat/attack vector addressed by the control does not exist), the licensee shall provide documentation that justifies why the control is not required; and demonstrates that the threat/attack vector does not exist. (NEI (A 3.1.6) RG (A 3.1.6))"

The Cyber Security Rule requires implementation of security controls to protect the identified assets from cyber attacks (10 CFR 73.54(c)(1)). ~~In the application of an actual Cyber Security program, a Cyber Threat/Attack vector is a means, channel, mechanism, or mode that uses a specific threat/attack pathway through which a known vulnerability can be exploited, using cyber means (e.g., to cause manipulation, and/or reconfiguration, and/or alteration of the device's software and/or data), to initiate or introduce a cyber attack on a CS or a CDA (Reference 1). The NRC has defined the Threat/Attack pathways in Section 6.1 of the Cyber Security Significance Determination Process (SDP) (Reference 2). This section in the SDP provides the five threat/attack vectors and specific questions that, if answered in the affirmative, identify that the pathway could be used to stage a cyber attack on a CS/CDA. The five threat/attack pathways described in this section are listed below:~~

~~a. Physical access to the CDA~~

~~b. Supply chain access to the CDA~~

~~c. Portable media/device connectivity to the CDA~~

~~d. Wired communications with the CDA~~

~~e. Wireless communications with the CDA~~

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6 (Reference 3, aka CSP)

provides a defensive strategy that consists of a defensive architecture and set of security controls that are employed to ensure the capability to detect, delay, respond to, and recover from cyber. ~~mitigate vulnerabilities and potential consequences of a cyber-attack staged through the threat/attack pathways~~. CSP Appendix A, Section 4.3 establishes the Defense-In-Depth protective strategies including the site defensive architecture. CSP Appendix A, Section 3.1.6.1 establishes the programmatic requirements for implementation of the Cyber Security Plan technical and operational controls. CSP Appendix A, Section 3.1.6.2 provides the programmatic controls for use of alternative cyber security controls/countermeasures. NEI 08-09, Revision 6, Addendum 1 (Reference 4) provides a revision to CSP Appendix A, Section 3.1.6.2 that aligns the evaluation of alternative counter measures CSP Appendix A, Section 3.1.6 to that required by 10 CFR 50.54(p). An excerpt of the revised CSP Appendix A, 3.1.6 is restated below:

> "For CDAs, the information in Sections 3.1.3–3.1.5 is utilized to analyze and document one or more of the following actions. NEI 13-10 may be used to satisfy the actions in 3.1.6.1.
>
> 1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.
>
> 2. Implementing alternative controls/countermeasures that mitigate the consequences of the threat/attack vector(s) associated with one or more of the cyber security controls enumerated in above by:
>
>   a. Documenting the basis for employing alternative countermeasures.
>
>   b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures mitigate the threat/attack vector the control is intended to protect.
>
>   c. Implementing alternative countermeasures determined in Section 3.1.6.2.b.
>
> 3. Not implementing one or more of the cyber security controls by:
>
>   a. Performing an analysis of the specific cyber security controls for the CDA that will not be implemented.
>
>   b. Documenting justification demonstrating the attack vector does not exist (i.e., not applicable) thereby demonstrating that those specific cyber security controls are not necessary."

3 ALTERNATIVE / APPLICABILITY JUSTIFICATIONS

In determining whether an alternative control/countermeasure being applied to a CDA mitigates the threat/attack vector the control is intended to protect, the evaluation should documented as required by CSP Appendix A, Section 3.1.6.2.~~address the following elements. During an inspection, if asked to provide documentation on an alternative control implementation, the licensee should consider providing a written response that addresses the following elements:~~

~~1.~~ ~~Identify and document the basis for whether or not each of the five threat/attack pathways has threat/attack vector(s) that are applicable to the CDA. This can be accomplished through a review of the Cyber Security SDP, Section 6.1 and using that review to answer each question (Reference 2). The questions from the Cyber Security SDP, Section 6.1 are provided below. For an existing CDA, this part of the evaluation should already have been done for the original assessment, but the following questions may assist in providing additional detail:~~

~~a.~~ ~~Physical access to the CDA.~~

~~Is physical access to and manipulation of the CS/CDA or use of the CS/CDA's HMI possible by personnel other than those with access authorization?~~

~~b.~~ ~~Supply chain access to the CDA.~~

~~Are vendor-provided software patches and updates installed without prior validation and testing on a separate support system or test bed contrary to the licensee's CSP?~~

~~Is the CS/CDA vendor permitted to have remote access to the CS/CDA for support purposes without cyber and physical end-point security?~~

~~Are there any system and services acquisition requirements that have not been implemented in accordance with the licensee's CSP?~~

~~c.~~ ~~Portable media/device connectivity to the CDA.~~

~~Can any form or format of portable electronic storage media be connected to or mounted on a media drive and utilized by the CS/CDA?~~

~~Can any form of portable computer/intelligent device be connected to and intercommunicate with the CS/CDA?~~

~~d.~~ ~~Wired communications with the CDA.~~

~~Does the CS/CDA have an enabled communications adapter with a connection to any type of local area network (LAN) or wide area network (WAN)?~~

~~Does the CS/CDA have an internal or external modem with a connection to a leased or public switched telephone network (PSTN) over which communication can transit?~~

~~Does the CS/CDA have a point-to-point (multi-point) synchronous or asynchronous serial communications link to another computer?~~

~~e. Wireless communications with the CDA.~~

~~Does the CS/CDA have any type of enabled wireless communications adapter (including infrared)?~~

2. Identify and explain the mitigation of the applicable threat/attack vector(s) (i.e., cyber security protection) provided by the original control that the alternative control is proposed to replace.

3. Explain how the alternative control/countermeasure mitigates each of the threat/attack vector(s) determined to be protected by the original control. The explanation needs to show how the security objective of the original control is met. ~~The justification may entail a combination of an alternative countermeasure plus other controls to mitigate the threat/attack pathway~~.

4. If the alternative control/countermeasure is confirmed to mitigate each of the threat/attack vector(s) the original control is intended to protect, then the documentation should become a portion of the assessment record for the CDA.

5. Implement the alternative control/countermeasure per CSP Appendix A, Section 3.1.6.2.c.

In the determination whether a specific cyber security control for the CDA will not be implemented, the functional capabilities of the CDA must be determined. Based on this determination, if the CDA does not have functional capabilities and if the functional capabilities cannot be introduced as a result of cyber compromise, then the attack vectors/threats associated with those functional capabilities of the CDA do not exist. Therefore, the security controls that protect against the attack vectors/threats associated with those functional capabilities can be addressed by documenting that the CDA does not have the functional capabilities and the functional capabilities cannot be introduced as a result of cyber compromise. ~~a similar process for determining the applicable threat/attack vectors should be used. Th the attack vectors/threats associated with that functional capabilities e evaluation should include the following:~~

~~1. Identify and document the basis for whether or not each of the five threat/attack pathways has threat/attack vector(s) that are applicable to the CDA. This can be accomplished by answering each of the questions in the Cyber Security SDP, Section 6.1. For an existing CDA, this part of the evaluation should already have been done for the original assessment, but the following items may assist in providing additional detail.~~

~~2. Identify and explain the mitigation of the applicable threat/attack vector(s) (i.e., cyber security protection) provided by the original control that the alternative control is proposed to replace.~~

~~3. If a threat/attack vector does not exist for a CDA, then the cyber security control that protects the non-existing vector does not need to be implemented for the CDA.~~

~~4. The documentation generated for this evaluation should become a portion of the assessment record for the CDA.~~

4 REFERENCES

1. Security Frequently Asked Questions (SFAQ) 16-06, “Communications Attack Pathways,” dated May 3, 2017

2. NRC Inspection Manual Chapter 0609, Appendix E, Part IV, “Cyber Security Significance Determination Process for Power Reactors,” dated August 15, 2017.

3. NEI 08-09, “Cyber Security Plan for Nuclear Power Plants,” Revision 6, dated April 2010

4. NEI 08-09, “Cyber Security Plan for Nuclear Power Plants,” Revision 6, Addendum 1, dated February 2017

5. NRC Inspection Procedure 71130.10P, “Cyber Security,” dated May 15, 2017