WHITE PAPER

NEI White Paper: Ongoing Monitoring and Assessment

Prepared by the Nuclear Energy Institute
July 2023

Acknowledgements

This document was developed by the Nuclear Energy Institute. NEI acknowledges and appreciates the contributions of NEI members and other organizations in providing input, reviewing and commenting on the document including:

NEI Project Lead:

Dave Feitl

Technical Lead:

Tony Lowry – Ameren Missouri

Member Support:

Scott Junkin – Southern Nuclear Operating Company

Adam Goodman – Duke Energy Corporation

Steve Flickinger – Constellation Energy Generation, LLC

Executive Summary

The regulation specified in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," provides requirements for the protection of nuclear power plants against cyber attacks. Licensees are required to identify assets requiring protection, implement security controls to protect identified assets, and to establish, implement, and maintain a cyber security plan that must be reviewed and approved by the Nuclear Regulatory Commission (NRC). NEI 08-09, Revision 6, "Cyber Security Plan for Power Reactors" provides a template for a cyber security plan and provides a catalog of cyber security controls. The cyber security plan and certain cyber security controls include a frequency for which some action is performed to maintain the effectiveness of the program. This document provides guidance and examples on tailoring these frequencies consistent with the Commission approved Cyber Security Plan.

Table of Contents

1 INTRODUCTION

1.1 Purpose

This document provides guidance and examples to licensees on the implementation of Ongoing Monitoring and Assessment (OMA) commitments and the tailoring of cyber security control frequencies (periodicities) as described in Appendix A, 3.1.6.2.d, NEI 08-09, Revision 6, “Cyber Security Plan for Power Reactors.”

1.2 Cyber Security Plan Control Periodicity Commitments

Periodicities in the Cyber Security Plan (CSP) are described in one of two categories:

1. Periodicities associated with the NEI 08-09 Appendix D and E controls; and
2. Periodicities which are implicit or explicit in the NEI 08-09 Appendix A Cyber Security Plan Template, such as:
    - Ongoing Monitoring and Assessment (CSP section 4.4);
    - Ongoing Assessment of Cyber Security Controls (CSP section 4.4.3); and
    - Effectiveness Analysis (CSP section 4.4.3.1).

Performing a periodic task at the specified frequency mitigates the threat addressed by the control. In accordance with CSP 3.1.6.2, implementing an alternate control, which has a similar periodic requirement and addresses the associated threat, satisfies the intent of the control. Alternatively, additional controls that mitigate the impact of the associated threat allow the frequency of the specified periodic task to be extended.

1.3 Applicability of Periodic Cyber Security Controls

NEI 13-10, "Cyber Security Control Assessments," defines a graded approach for classifying CDAs based upon the functions they perform and the capabilities of digital devices. Non-direct CDAs have defined minimum baseline attributes which may include only a subset of periodic cyber security controls. Low functioning (non-complex) direct CDAs may only comprise a subset of the technical periodic cyber security controls. For low-functioning CDAs, where the attack vector is negated by its design, OMA cyber security controls are not applicable and should be documented as part of the evaluation.

1.4 Basis for Adjustment of Control Periodicity (3.1.6.2)

Section A.3.1.6 of the CSP, “Mitigation of Vulnerabilities and Application of Cyber Security Controls,” provides three approaches to the analysis and documentation of cyber security controls for CDAs. Additional guidance is described in Sections 1.4.1 – 1.4.3 below.

1.4.1 Perform as Written

The first approach, as described in Section 3.1.6.1 of the CSP, is to “Implement the Cyber Security Controls in Appendices D and E of NEI 08-09, Revision 6.” This option does not provide for a modification

to the controls in Appendices D and E. This language commits the licensee to implement the security controls in Appendices D or E as written; and any modification to the elements of the control creates an alternate control. **Therefore, if the control periodicity is adjusted, the implementation of the control does not satisfy this option.**

1.4.2 Alternate Controls/Countermeasures

The second approach is when a security control is not implemented as described. If any element (including the periodicity) of a security control is altered, the commitments of Section 3.1.6.1 are not satisfied. Therefore, the control is considered as an alternate control, and must satisfy all of the elements of Section 3.1.6.2, including the basis for the use of an alternate periodicity. Section 3.1.6.2.d provides licensees with the method to justify the implementation of an alternate frequency or periodicity:

NEI 08-09, Appendix A, Section 3.1.6.2

1. *Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) 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 provide the same or greater cyber security protection as the corresponding cyber security control; and*

    c) *Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control;*

    d) *Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:*

        i. *NRC Regulations, Orders*

        ii. *Operating License Requirements (e.g., Technical Specifications)*

        iii. *Site operating history*

        iv. *Industry operating experience*

        v. *Experience with security control*

        vi. *Guidance in generally accepted standards (e.g., NIST, IEEE, ISO)*

        vii. *Audits and Assessments*

        viii. *Benchmarking*

        ix. *Availability of new technologies.*

Licensees that have amended their CSP to include Addendum 1 to NEI 08-09 can use the following method for implementing an alternate periodicity:

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 (1) 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; and*

    c) *Implementing alternative countermeasures determined in Section 3.1.6.2.b;*

    d) *Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:*

        i. *NRC Regulations, Orders*

        ii. *Operating License Requirements (e.g., Technical Specifications)*

        iii. *Site operating history*

        iv. *Industry operating experience*

        v. *Experience with security control*

        vi. *Guidance in generally accepted standards (e.g., NIST, IEEE, ISO)*

        vii. *Audits and Assessments*

        viii. *Benchmarking*

        ix. *Availability of new technologies.*

Section 3.1.6.2.d provides licensees with the method for implementing an alternate periodicity that is supported by one or more of the nine bases for the alternate. However, no guidance was provided on how these bases can be applied for a change in periodicity. The bases for this guidance is now described in Section 2 of this document.

1.4.3 Analysis Determining Attack Vector Does Not Exist

The third approach as described in Section 3.1.6.3 is to perform an analysis of the CDAs and associated controls and to document the justification demonstrating the attack vector doesn't exist, providing evidence that the specific cyber security controls aren't necessary. **Therefore, implementing an alternate periodicity would not apply.**

2 ALTERNATE FREQUENCY OR PERIODICITY BASES

2.1 Bases Guidelines

NEI 08-09, Section 3.1.6.2.d provides for implementing an alternate frequency or periodicity associated with a security control by documenting the basis for the alternative.

An effective basis for changing the periodicity of a security control could include an assessment, justification, and implementation of alternate activities. These alternate activities may have a periodicity, or may be alternate security controls that mitigate risk associated with the threat vector by providing additional protections.

In some cases, the alternate activities will either meet or exceed the periodicity of the original cyber security control. In other cases, licensees can use the criteria in this guidance to change the periodicity of the security control based on the reduced attack vector. By meeting the criteria, it is acceptable to modify the periodicity of the security controls described in the Appendices D and E of NEI 08-09 Rev. 6, “Cyber Security Plan for Nuclear Power Reactors.”

Through site operating history, industry operating experience, experience with the security controls, and benchmarking, justifications that may be used to alter the frequency of the periodic security controls include:

- OMA activities are aligned with regularly scheduled maintenance or Out of Service times for the CDA to minimize the operational and nuclear safety risk of adversely impacting the CDA function while in an operating condition
- CDA is located in a continuously manned area
- CDA is in a locked, tamper sealed, or alarmed enclosure
- Security or Operator rounds cover the area where the CDA is located at a frequency that is more conservative than the specified periodicity
- CDA is connected to a cyber security monitoring system (IDS/SIEM) and generates alerts for defined activities
- Device functionality is tested frequently

In cases where interfacing with the CDA while in service or performing activities may disrupt the CDA function, licensees may align OMA activities with scheduled maintenance activities, licensee operational activities, or scheduled out of service times. For example, checking configuration settings or changing the device passwords. These actions may only be possible by taking the device out of service.

Frequency extensions beyond timeframes that are accommodated by regular maintenance intervals are very rare and must be supported by specific limiting conditions. Examples:

- Radiation safety (e.g., containment, high radiation area where the levels have recently increased, there is information that the high radiation levels are not going to decrease any time soon, and it is not safe for personnel to enter the area)

- Unforeseen circumstances beyond the control of the licensee (e.g., unplanned or unexpected reactor trips, events)

- Extreme natural events (e.g., tornadoes, hurricanes, earthquakes, flooding that impacts the operation of the site)

The justification and circumstances must be documented.

2.2 Bases Justification Using NEI 08-09 Section 3.1.6

Potential justifications for frequency extensions can be extrapolated from the nine bases listed in Section 3.1.6.2.d.

2.2.1 Section 3.1.6.2.d.i NRC Regulations/Orders:

Licensees may consider activities performed to meet the requirements of the physical security program. For example, activities performed on a frequency or periodicity include (but are not limited to):

- Reviewing the unescorted access authorization list every 31 days and verifying personnel in the critical group to meet the requirements of 10 CFR 73.56, “Personnel Access Authorization Requirements for Nuclear Power Plants,”

- Conducting security patrols, testing intrusion detection systems, physically restricting access by utilizing the lock and key control program and reviewing personnel access, and;

- Performing surveillance with cameras.

Licensees may credit the periodicity at which these activities or attributes are performed to meet or exceed the periodicity of the cyber security control. Application includes security controls that mitigate the physical access and Portable Media and Mobile Devices (PMMD) attack pathways to the CDA. Licensees should document (e.g., CDA assessments, security control implementation strategy guidance, logs, or any other licensee record) and demonstrate these activities are in accordance with a periodicity meeting or exceeding the periodicity described in the cyber security control. This basis can be assumed to meet the already established regulatory requirements and therefore is satisfactory to provide adequate protection.

2.2.2 Section 3.1.6.2.d.ii Operating License Requirements (E.G., Technical Specifications):

If a control periodicity is in conflict with a licensing requirement or Technical Specification (TS), the licensee may use the license requirement as a basis for the implementation of an alternate control and/or periodicity.

In the absence of a conflict, the licensee may align the periodicity with TS surveillance, maintenance, or calibration requirements, provided that:

- There is a periodicity associated with the TS activity (e.g., the device is calibrated every 180 days) or other NRC approved document such as the physical security plan (PSP) or Emergency Plan (EP),

- The documentation associated with the TS activity (i.e., work orders) explicitly requires the completion and recording of the results of the periodic cyber security activity; and

- Personnel performing the activity are trained in the completion of the cyber security task.

Licensees may use a combination of Section 3.1.6.2.d.ii and ii as the basis for changing the periodicity of the security control. The periodicity may be extended for equipment that cannot be shutdown due to operational or nuclear safety challenges, or license conditions.

2.2.3 Section 3.1.6.2.d.iii Site Operating History

Through past performances of ongoing monitoring activities, sites may learn that some activities have more potential to create a risk to system function than is offset by the potential benefit of the activity.

Examples:

- A system with redundant servers required rebooting the servers to perform password changes. Due to a system resource issue and aging system, reboots would sometimes cause a virtual memory issue which could only be fixed by restoring the system from a backup image. This would result in deliberately placing the system in a degraded non-redundant condition on a periodic frequency.

- Connection of a keyboard to an aging system for baseline configuration checks caused a physical failure of the computer port which could not be repaired without removing the computer from a rack and taking it out of service.

- A firmware based speed controller requires taking the device out of service to access the menu for password changes or baseline configuration checks. Removing the device from service increases plant safety risk. Work is normally performed on the device only during refuel outages.

Consequently, frequencies should be adjusted to align periodic cyber security tasks with regularly scheduled maintenance to reduce risk. The same justification could apply to other cases where accessing or manipulating a device while in service could increase the risk of adversely impacting the SSEP function.

In similar instances, it may be prudent to use this adverse impact potential to justify alternate controls and/or extended frequencies. Licensees should also consider whether the CDA is included in the 10 CFR 50.65, “Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,”. Justification for alternate periodicity may be appropriate using the Maintenance Rule in order to limit potential out of service time.

2.2.4 Section 3.1.6.2.d.iv Industry Operating Experience

Operating experience is shared through industry calls, meetings, and documents. Often, issues encountered at one site may also apply to others.

Examples:

Password changes have been a common area with a potential to cause adverse impact to CDA function.

- In one case, a System Engineer incorrectly documented a new BIOS password before leaving the company. When access was needed to this device, the incorrect password was discovered and the device had to be removed from service to reset the BIOS jumper.

- In another example, a system owner failed to correctly set one of several system service passwords. This caused a service that automatically purges old records to fail and was not discovered until the system started having issues due to inadequate free space.

- In another case, a network switch password change was not documented properly for the administrator account and the switch had to be rebuilt to recover, resulting in system down time.

When allowed by alternate mitigating actions, it may be prudent to consider the potential adverse impact of performing password changes, especially for complex systems with multiple passwords, and use this justification to extend frequencies to reduce risk.

A licensee may use Industry Operating Experience as an acceptable method of justification for alternative periodicity when it applies to similar CDA configurations, but may need to be used in combination with additional basis justifications.

2.2.5 Section 3.1.6.2.d.v Experience with Security Control

As licensees have gained experience with security controls and their implementation, they have increased their knowledge regarding the purpose of the controls and the threat being addressed. When the intent of a control is understood, it is possible to implement additional actions to mitigate the associated threat.

For instance, site Configuration Management programs update CDA configuration documentation to reflect authorized changes. Methods of identifying unauthorized or malicious changes to a CDA include:

- Baseline configuration comparisons against documented hardware and software configurations

- Rogue connection checks

Additional controls reducing the threat, addressed by this periodic control, may be credited to define an extended frequency.

Example:

- Additional alerts could be created in the cyber security monitoring system (IDS/SIEM) to recognize specific conditions,

- Controls like application whitelisting could be implemented to greatly limit the ability for an individual to make unauthorized changes; and/or

- Device whitelisting or MAC address locking could mitigate the ability to connect unauthorized devices.

2.2.6 Section 3.1.6.2.d.vi Guidance in Generally Accepted Standards (E.G., NIST, IEEE, ISO)

The security controls in NEI 08-09 are based upon NIST 800-53 (Revision 3). NIST may update portions of their standards over time. Reviews of these changes may provide improved or alternate protection methods and/or justifications for altering existing frequencies. There are other NIST standards and other generally accepted standards in the nuclear industry and other industries that contain guidance applicable to the cyber security protection of devices and systems similar to site CDAs. These additional standards may assist licensees in developing justifications for alternate frequencies that meet the intent of current regulation or regulatory guidance. Licensees will need to document a clear link between other generally accepted standards and the alternate control basis justification.

2.2.7 Section 3.1.6.2.d.vii Audits and Assessments

Site Audits and Assessments may identify concerns with that site's implemented frequencies which may need adjustment. Similarly, audits and assessments of industry peers may identify an ongoing monitoring area needing evaluation or may reveal best practices that could be followed for similar frequency adjustments. Audits are a method to explore the 'why' behind the reason a periodicity is established and therefore the logic used in the audit finding would provide the basis for adjustment, rather than referencing the audit itself.

2.2.8 Section 3.1.6.2.d.viii Benchmarking

Benchmarking is a method for gathering Industry Operating Experience and should be documented in combination with the OE providing the acceptable justification.

2.2.9 Section 3.1.6.2.d.ix Availability of New Technologies

Implementation of new technologies, or adapting the application of existing technologies, may provide additional capabilities that may automate, replace, or mitigate the risks being addressed by ongoing monitoring tasks. As improvements are made to tools and techniques, there may be additional protections and monitoring capabilities that mitigate the threats being addressed by the ongoing monitoring activities.

For example:

- Tools that monitor installed applications and configurations may prevent the ability for unauthorized programs to run or unauthorized system changes to be made.

- The creation of additional log monitoring queries and alerts for certain types of activities may warn the cyber security team when specified undesirable activities occur.

These improved capabilities may justify the extension of some periodic activities due to the improved mitigation of the threat.

Cybersecurity tools and protection methodologies continually evolve and are replaced. In some cases, a vendor may discontinue support for an existing product or method of performing a task. For example, many products are migrating to the cloud and vendors are discontinuing support for performing offline signature updates or stand-alone device scans. Similarly, system upgrades to improve safety and reliability may utilize vendor supplied proprietary applications developed for legacy operating systems

that are no longer supported. It may not be possible to continue performing an ongoing monitoring task (e.g., signature updates, scans, vulnerability assessments, etc.) until the system or device is upgraded to a supported platform. Lifecycle management and engineering modifications, with well-documented justification, could be considered under this basis of justification. This justification would recognize that the best way to mitigate a CDA's threat vector is to replace or modify the CDA. In this instance, with reasonable change management strategies in place, a basis justification could be used to provide adequate alternate periodicities until the device can be upgraded or replaced.

3 GENERAL EXAMPLES OF ALTERNATE CYBER SECURITY CONTROL PERIODICITIES OR FREQUENCIES

Example #1: Documented periodic (once per shift) patrols of vital areas or daily security officer insider mitigation program (IMP) and operator rounds are used to satisfy 10CFR73.55 Physical Security program requirements AND security officers who perform these patrols are trained and required by procedure to surveil tamper seals placed over unused ports on CDAs that are located in the vital area AND the procedure provides for an adequate reporting system should there be detection of tampering.

This alternate control addresses the physical access and PMMD attack vectors associated with the D.1.18 Insecure and Rogue Connections, AND the implemented periodicity of this control exceeds the periodicity prescribed by D.1.18. Therefore, these patrols can be credited as an alternate control with an alternate periodicity to the D1.18 Insecure and Rogue Connections control and periodicity.

Example #2: Taking credit for the CDA's connection to the cyber security monitoring system (IDS/SIEM) to mitigate the possibility of an individual making unauthorized changes to the CDA configuration could allow for less frequent baseline configuration checks, or justify a methodology of performing baseline configuration reviews against a sample of CDAs each review period.

Centralized monitoring systems allow for the analysis of CDA logs or network traffic to identify and alert on unusual activities. This mitigates the possibility of an individual making unauthorized changes to the CDA configuration. Therefore, credit may be taken for the continuous monitoring and alerting to align the cyber security control periodicities with other activities normally performed on the CDA. A similar case could be made for CDAs employing application whitelisting.

Example #3: Passwords ensure only authorized individuals have access to CDAs and privileged functions. Access to CDAs can also be limited to authorized individuals by locating CDAs inside cabinets that are alarmed or locked and key controlled with authorized access limited to the critical group.

The cabinet key is under a key control program that is verified or audited on an established periodic basis.

Individuals with physical and logical access to the CDA have been granted access under the 10 CFR 73.56 Access Authorization Program and continue to meet the periodic Behavioral Observation Program (BOP) and Fitness-for-Duty (FFD) requirements.

Therefore, the additional security controls mitigate unauthorized access and allow the periodicity of password changes to be extended. Password changes should still also be assessed based on events, such as personnel changes, to ensure that only personnel with a need have access to CDAs.

Example #4: Device whitelisting or MAC address locking block rogue devices connected to the network from communicating. Centralized cyber security monitoring can detect and alert on new network connections. Application of these security controls mitigates the threat from rogue connections.

Therefore, the frequency for performing rogue connection checks may be extended.

Example #5: A licensee implements a technology that provides real-time detection of devices which connect to network infrastructure. The alternate control is intended to address the periodic frequency associated with the D.1.17 Wireless Access Restrictions control and the CSP Appendix A 4.4 which prescribes that the licensees perform ongoing monitoring to verify “that rogue assets are not connected to the network infrastructure.” The real-time detection provided by the alternate control exceeds the original control frequency. However, it would be appropriate to implement a periodic test of the real-time detection technology to ensure it continues to satisfy the periodic frequency for the original control.