NUCLEAR ENERGY INSTITUTE
1201 F Street NW • Suite 1100
Washington, DC 20004
nei.org

Richard Mogavero
Director, Incident Preparedness
Technical & Regulatory Services

Phone: 202.739.8174
Email: rm@nei.org

April 7, 2025

Mr. Mario Fernandez
Cybersecurity Branch Chief, Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Endorsement of NEI 08-09, Revision 7, "Cyber Security Plan for Nuclear Power Reactors"

Project Number: 689

Dear Mr. Fernandez:

The Nuclear Energy Institute (NEI)[1], on behalf of its members, is submitting NEI 08-09, Revision 7, *Cyber Security Plan for Nuclear Power Reactors*, dated April 7, 2025, for NRC review and endorsement. This revision has been developed in collaboration with NEI member companies to update and clarify guidance supporting licensee cyber security programs under 10 CFR 73.54, *Protection of Digital Computer and Communication Systems and Networks*.

This revision also incorporates NRC feedback from two public meetings[2] and includes clarifications on cybersecurity fundamentals, such as threat and vulnerability management, wireless technologies, defense-in-depth, alternate controls, and critical group criteria. These clarifications will enhance consistency across the industry.

NEI requests that the NRC complete its review and provide endorsement of NEI 08-09, Revision 7 under the fee exemption granted on January 17, 2023[3].

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

[2] ML24165A217 - 06/25/2024 Notice of Meeting with the Nuclear Energy Institute (NEI) / ML25042A456 - 02/25/2025 Notice of Meeting with the Nuclear Energy Institute (NEI)

[3] Fee Exemption Request for NEI 08-09 Revision 7, "Changes to NEI 08-09 Cyber Security Plan for Nuclear Power Reactors" (ML22348A112)

If you have any questions or require additional information, please contact Chance Siri at cms@nei.org, or me.

Sincerely,

Rich Mogavero
Director, Security & Incident Preparedness

c: Mr. John McKirgan, NSIR/DPCP, NRC
NRC Document Control Desk

Attachment(s):
NEI 08-09, Revision 7, “Cyber Security Plan for Nuclear Power Reactors”

NEI 08-09 [Rev. 7]

Cyber Security Plan for Nuclear Power Reactors

2025

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

NEI 08-09 [Rev. 7]

Nuclear Energy Institute

Cyber Security Plan for Nuclear Power Reactors

April 2025

Nuclear Energy Institute, 1201 F Street NW, Washington D.C.

ACKNOWLEDGEMENTS

This document has been prepared by the nuclear power industry with input and guidance from the United States Nuclear Regulatory Commission.

Contributors to this manual include:

Janardan Amin	Luminant Power
Jim Andersen	Excel Services Corporation
Sandra Bittner	Arizona Public Service Company
Cynthia Broadwell	Progress Energy
Steve Carr	Florida Power & Light Company
Larry Cerier	Exelon Corporation
Michael Dack	Constellation Energy Corporation
Jeff Drowley	Exelon Corporation
Nathan Faith	American Electric Power Company
Dave Feitl	Xcel Energy Inc.
Steve Flickinger	Constellation Energy Corporation
Steve Foley	Exelon Corporation
Glen Frix	Duke Energy Corporation
Jan Geib	South Carolina Electric & Gas Company
Matt Gibson	Progress Energy
Bob Gill	Duke Energy Corporation
Adam Goodman	Duke Energy Corporation
William Gross	NEI
Scott Junkin	Southern Nuclear Operating Company
Glen Kaegi	Exelon Corporation
Tony Lowry	Ameren Corporation
Brian Miller	Progress Energy
Jerry Mills	TerraPower LLC
Rich Mogavero	NEI
Ryan Moss	South Texas Project Nuclear Operating Company
Phil Prugnarola	Florida Power & Light Company
Jack Roe	NEI
Ron Rose	FirstEnergy Corporation
Geoff Schwartz	Entergy
Chance Siri	Pacific Gas & Electric Company
George Sisley	Vistra Corporation
Douglas Walker	Exelon Corporation
Brad Yeates	Southern Nuclear Operating Company

NOTICE

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

EXECUTIVE SUMMARY

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

Licensees are required to protect digital computer and communications systems and networks performing the following categories of functions from those cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data and/or software; deny access to systems, services, and/or data, and; impact the operation of systems, networks, and associated equipment:

(i) Safety-related and important-to-safety functions;
(ii) Security functions;
(iii) Emergency preparedness functions, including offsite communications; and
(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

10 CFR 73.54 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan.

10 CFR 73.54 requires that licensees and applicants establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of the Rule. The Rule states:

(1) The cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.
(2) The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will:

(i) Maintain the capability for timely detection and response to cyber attacks;
(ii) Mitigate the consequences of cyber attacks;
(iii) Correct exploited vulnerabilities; and
(iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

This document was developed to assist licensees in constructing and implementing their Cyber Security Plan license submittal as required by 10 CFR 73.54.

TABLE OF CONTENTS

CYBER SECURITY PLAN FOR NUCLEAR POWER REACTORS

1 INTRODUCTION

1.1 BACKGROUND

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

10 CFR 73.54 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan.

Further, 10 CFR 50.34(c)(2) states in part that "Each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54 of this chapter." The Cyber Security Plan establishes the licensing basis for the Cyber Security Program.

The purpose of the Cyber Security Plan (Plan) is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented. The intent of the Plan is to protect the health and safety of the public from radiological sabotage as a result of a cyber attack as described in 10 CFR 73.1. 10 CFR 50.34(c), "Physical Security Plan," requires the inclusion of a physical security plan.

NEI 04-04 Revision 1 provided an industry response using a programmatic approach to the NRC cyber security Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," February 2002. In a letter dated December 23, 2005, the NRC found that NEI 04-04, Revision 1, dated November 18, 2005, was, "an acceptable method for establishing and maintaining a cyber security program at nuclear power plants." NEI 04-04 Rev. 1 provided a foundation for a Cyber Security Program for US Power Reactors. The actions taken by the industry in this binding initiative were implemented at all operating US nuclear power reactors with NRC endorsement and remain the foundation for the industry's current Programs. NEI 04-04 Revision 1 has not been accepted by the NRC to meet the requirements of 10 CFR 73.54.

NEI 08-09 describes a defensive strategy that consists of a defensive architecture and set of security controls that are based on the NIST SP 800-82, Final Public Draft, Dated September 29, 2008, "Guide to Industrial Control System Security," and NIST SP 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems" standards. The security controls contained in NEI 08-09 Appendices D and E are tailored for use in nuclear facilities and are based on NIST SP 800-82 and NIST SP 800-53. Licensees may leverage newer versions of

the cited NIST guidance in their entirety where the guidance provides more clarity per the purpose of the control.

1.2 PURPOSE

NEI 08-09 has been developed to assist licensees in complying with the requirements of 10 CFR 73.54.

2 CYBER SECURITY PLAN PREPARATION

NEI 08-09, Revision 7 contains the following guidance and resources:

Appendix A – Cyber Security Plan Template – This template should be used by licensees to develop the cyber security plan that must be submitted to the NRC pursuant to 10 CFR 73.54. Information contained in brackets must be revised as necessary with licensee specific information and the brackets removed. Other licensee-specific information includes the defensive strategy. Changes to other portions of the template should be avoided. The submitted plan will reference Appendices B, D, and E, as appropriate. Page numbers of the template should be revised to read 1, 2, 3, etc. rather than A-1, A-2, A-3, etc.

Appendix B – Glossary – A glossary of terms used in NEI 08-09. These terms reference established and reliable sources and should not be revised.

Appendix C – [deleted]

Appendix D – Technical Security Controls – Technical controls are the countermeasures implemented to protect the availability, integrity, and confidentiality of a system. The measures employed are designed to protect against unauthorized access, use, disruption, modification, or destruction of a CDA and/or its function. System level controls are used individually, or in combination with other countermeasures, methods, or techniques to provide protective barriers for identified risks. Technical controls are tested, evaluated for effectiveness, monitored, replaced, or supplemented as required to ensure a security level to mitigate identified risks.

Appendix E – Management and Operational Controls – Management and operational cyber security controls are carried out by including cyber security enhancing activities in policies, implementing procedures, and processes such as engineering lifecycle activities, engineering procurement procedures, Software Quality Assurance program, and ensuring procurement contracts specify cyber security requirements.

Addenda 2 through 5 – Provides additional implementation guidance for specific sections in this document.

APPENDIX A: CYBER SECURITY PLAN TEMPLATE

CYBER SECURITY PLAN FOR
[SITE/LICENSEE]

1 INTRODUCTION

The purpose of this Cyber Security Plan (Plan) is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented at [site(s)]. The intent of this Plan is to protect the health and safety of the public from radiological sabotage as a result of a cyber attack as described in 10 CFR 73.1. 10 CFR 50.34(c), "Physical Security Plan," requires the inclusion of a physical security plan. [Site/Licensee] acknowledges that the implementation of this plan does not alleviate their responsibility to comply with other NRC regulations.

Further, 10 CFR 50.34(c)(2) states in part that "Each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54 of this chapter." This Cyber Security Plan establishes the licensing basis for the Cyber Security Program (Program) for [site(s)]. [Elements of the Program described in this Plan are applicable to all sites unless otherwise stated.]

A Glossary of terms used within this Plan and Appendices of NEI 08-09, Revision 7, is contained in Appendix B of NEI 08-09, Revision 7.

2 CYBER SECURITY PLAN

2.1 SCOPE AND PURPOSE

This Plan establishes a means to achieve high assurance that digital computer and communication systems and networks associated with the following functions (hereafter designated as Critical Digital Assets (CDAs)) are adequately protected against cyber attacks up to and including the Design Basis Threat (DBT) as described in 10 CFR 73.1:

1. Safety-related and important-to safety functions;
2. Security functions;
3. Emergency preparedness functions including offsite communications; and
4. Support systems and equipment which if compromised, would adversely impact safety, security, or emergency preparedness functions.

The safety-related and important-to safety functions, security functions, and emergency preparedness functions including offsite communications are herein referred to as SSEP functions.

High assurance of adequate protection of systems associated with the above functions from cyber attacks is achieved by:

1. Implementing and documenting the "baseline" cyber security controls described in Section 3.1.6 of this Plan; and
2. Implementing and documenting a cyber security program to maintain the established cyber security controls through a comprehensive life cycle approach as described in Section 4 of this Plan.

2.2 PERFORMANCE REQUIREMENTS

10 CFR 73.55(a)(1) requires that licensees implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plans, and Cyber Security Plan, referred to collectively as "security plans."

As required by 10 CFR 73.54(b)(3), cyber security is a component of the physical protection program. As such, this Plan establishes how digital computer and communication systems and networks within the scope of 10 CFR 73.54 are adequately protected from cyber attacks up to and including the DBT characteristics described in RG 5.69, "Guidance for the Application of the Radiological Sabotage Design Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements." (Safeguards Information (SGI))

Performance based requirements demonstrated in this Plan are designed to:

2.2.1 Evaluate modifications to CDAs prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBT. (10 CFR 73.54(a)(1) and 10 CFR 73.54(d)(3)).

2.2.2 Prevent adverse impact to SSEP functions resulting from cyber attacks, that would adversely impact the integrity or confidentiality of data and/or software, deny access to systems, services, and/or data, and adversely impact the operation of systems, networks, and associated equipment to protect against the DBT. (10 CFR 73.54(a)(2) and 10 CFR 73.55(b)(2))

2.2.3 Analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attack to preserve the intended function of plant systems, structures, and components within the scope of the Rule and account for these conditions in the design of the Program. (10 CFR 73.54(b)(1) and 10 CFR 73.55(b)(4)).

2.2.4 Establish, implement and maintain the Program in accordance with 10 CFR73.54. (10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8)).

2.2.5 Incorporate the cyber security program as a component of the physical protection program. (10 CFR 73.54(b)(3) and 10 CFR 73.55(b)(8)).

2.2.6 Implement security controls to protect the identified assets from cyber attacks (10 CFR 73.54(c)(1))

2.2.7 Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the Program.
(10 CFR 73.54(c)(2) and 10 CFR 73.55(b)(3)(ii)).

2.2.8 Maintain the capability to mitigate the adverse consequences of cyber attacks.
(10 CFR 73.54(c)(3) and 10 CFR 73.54(e)(2)(ii)).

2.2.9 Ensure that the functions of identified protected assets are not adversely impacted due to cyber attacks. (10 CFR 73.54(c)(4))

2.2.10 Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities. (10 CFR 73.54(d)(1)).

2.2.11 Use the site corrective action program to: 1) track, trend, correct, and prevent recurrence of cyber security failures and deficiencies, and 2) evaluate and manage cyber risks. (10 CFR 73.54(d)(2) and 10 CFR 73.55(b)(10)).

2.2.12 Describe how the cyber security program requirements will be implemented; accounting for the site-specific conditions that affect implementation.
(10 CFR 73.54(e)(1))

2.2.13 Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in 10 CFR73.1
(10 CFR 73.54(e)(2)(i), 10 CFR 73.54(e)(2)(iv) and 10 CFR73.55(b)(2)).

2.2.14 Maintain the capability to correct exploited vulnerabilities.
(10 CFR73.54(e)(2)(iii)).

2.2.15 Demonstrate the ability to meet Commission requirements through implementation of the Program in licensee policies and procedures which are available upon the request of an authorized representative of the Commission.
(10 CFR 73.54(f) and 10 CFR 73.55(b)(5)).

2.2.16 Review the cyber security program as a component of the physical security program, including the periodicity requirements.
(10 CFR 73.54(g) and 10 CFR 73.55(m)).

2.2.17 Describe how all records and supporting technical documentation are retained.
(10 CFR 73.54(h)).

2.2.18 Coordinate implementation of this Plan and associated procedures with other [site/fleet] procedures to preclude conflict during both normal and emergency conditions. (10 CFR 73.55(b)(11)).

3 ANALYZING DIGITAL COMPUTER SYSTEMS AND NETWORKS

The Cyber Security Program is established, implemented and maintained in accordance with 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8) to protect those systems required by 10 CFR 73.54(a)(1)(i–iv) from cyber attacks that would: adversely impact the integrity or confidentiality of data and/or software; deny access to systems, services and/or data; or adversely impact the

operation of systems, networks, and associated equipment. This Cyber Security Program complies with 10 CFR 73.54 by implementing cyber security controls, defensive strategies, and attack mitigation methods that meet the Rule.

The cyber security controls described in Appendices D and E of NEI 08-09, Revision 7, are implemented in accordance with Section 3.1.6 of this Plan. Documentation of the cyber security controls in place for CDAs are not submitted with this Plan but are available on site for inspection by the NRC. Cyber security program changes that are determined to decrease the effectiveness of this Plan are submitted to the NRC for approval as required by 10 CFR 50.90. Revisions to this Plan are processed in accordance with procedures that implement the requirements of 10 CFR 50.54(p). Cyber attacks at [Site] are reported to the NRC in accordance with the requirements of 10 CFR 73.77.

3.1 ANALYZING DIGITAL COMPUTER SYSTEMS AND NETWORKS AND APPLYING CYBER SECURITY CONTROLS

In accordance with 10 CFR 73.54(b)(1), the Cyber Security Program is established, implemented, and is maintained to:

- Analyze digital computer and communications systems and networks, and
- Identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

In accordance with 10 CFR 73.54(c)(1), cyber security controls are implemented to protect the assets identified by 10 CFR 73.54(b)(1) from cyber attacks. The cyber security controls provided in Appendices D and E of NEI 08-09, Revision 7 are used as the basis for protecting the identified CDAs.

Cyber security risks are evaluated, managed, and mitigated to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the DBT. The cyber security controls provided in Appendices D and E of NEI 08-09, Revision 7 are the technical, operational, and management countermeasures available to protect the availability, integrity, and confidentiality of CDAs. The cyber security controls in Appendices D and E of NEI 08-09, Revision 7 are implemented using the methodology in Sections 3.1.1 through 3.1.6 below. In so doing, high assurance of adequate protection of CDAs associated with SSEP functions from cyber attacks defined by 10 CFR 73.1 and RG 5.69 is ensured.

3.1.1 Cyber Security Assessment and Authorization

[Site/Licensee] develops, disseminates, periodically reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, cyber security assessment and authorization [policy/procedure] that defines and addresses: the purpose, scope, roles, responsibilities, management commitment, and coordination among [departments]; and the implementation of the cyber security controls in Appendices D and E of NEI 08-09, Revision 7.

- A formal, documented procedure to facilitate the implementation of the cyber security assessment.

3.1.2 Cyber Security Assessment Team

A Cyber Security Assessment Team (CSAT) is formed consisting of individuals with broad knowledge in the following areas:

- Information and digital system technology – This includes cyber security, software development, offsite communications, computer system administration, computer engineering and computer networking. Knowledge of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant information systems, is included. Plant operational systems include programmable logic controllers, control systems, and distributed control systems. Information systems include computer systems and databases containing information used to design, operate, and maintain CDAs. In the networking arena, knowledge of both plant- and corporate-wide networks is included.
- Nuclear power plant operations, engineering, and nuclear safety – This includes overall facility operations and plant technical specifications. The staff representing this technical area has the ability to trace the impact of a vulnerability or series of vulnerabilities in a CDA (or connected digital asset) outward through plant systems and subsystems so that the overall impact on SSEP functions of the plant can be evaluated.
- Physical security and emergency preparedness – This includes the site's physical security and emergency preparedness systems and programs.

The roles and responsibilities of the CSAT include such activities as:

- Performing or overseeing stages of the cyber security assessment process.
- Documenting key observations, analyses, and findings during the assessment process.
- Evaluating assumptions and conclusions about cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs and cyber security controls throughout their system life cycles; and estimates of cyber security risk levels.
- Confirming information acquired during tabletop reviews by conducting walk-downs or electronic validation of CDAs and connected digital assets and associated cyber security controls.
- Identifying potential new cyber security controls.
- Documenting the required cyber security control application per Section 3.1.6 of this Plan.
- Transmitting assessment documentation, including supporting information, to Records Management in accordance with 10 CFR 73.54(h) and the record retention requirements specified in Section 4.13 of this Plan.

The CSAT has the authority to conduct an assessment in accordance with the requirements of Section 3 of this Plan.

3.1.3 Identification of Critical Digital Assets

The CSAT:

- Identifies and documents Critical Systems (CS), which must be protected under the Rule. (Refer to NEI 08-09, Revision 7, Appendix B, Glossary for definition of Critical System)
- Identifies and documents Critical Digital Assets (CDAs). (Refer to NEI 08-09, Revision 7, Appendix B, Glossary for definition of Critical Digital Asset)

The process by which CDAs are identified has been documented.

For each CS examined, the documentation includes the following:

- Identification of the Critical System;
- Identification of the digital devices that provide direct or supporting roles in the function of the CS (e.g., protection, control, monitoring, reporting, or communications);
- Identification of CDAs within the Critical System;
- General description of the CDAs;
- Brief description of overall function of the CDAs;
- Description of overall consequence to the CS and SSEP functions if a compromise of the CDA occurs; and
- Security functional requirements or specifications, as available, that include the following:
  - Information security requirements necessary for vendors and developers to maintain the integrity of acquired systems;
  - Secure configuration, installation, and operation of the CDA;
  - Effective use and maintenance of security features/functions;
  - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
  - User-accessible security features/functions and how to effectively use those security features/functions;
  - Methods for user interaction with CDAs, which enables individuals to use the system in a more secure manner; and
  - User responsibilities in maintaining the security of the CDA.

3.1.4 Examination of Cyber Security Practices

The CSAT collects, examines, and documents the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture

drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process. The team collects documents by reference and evaluates the following as they apply to CDAs:

- Site- and corporate-wide information on defensive strategies including cyber security controls, defensive models, and other defensive strategy measures;
- The site's physical and operational security program with respect to the protection of CDAs;
- Site and corporate network architectures, and configuration information on security devices;
- Cyber security requirements for vendors and contractors while on site or used during procurement;
- Information on computer networks and communication systems and networks that are present within the plant and could be potential pathways for attacks;
- Cyber security assessments, studies, evaluations or audits to gain insight into areas of potential vulnerabilities; and
- Infrastructure support systems (e.g., electrical power; heating, ventilation, and air conditioning (HVAC); communications; fire suppression) which, if compromised, could adversely impact the proper functioning of CDAs.

The examination includes an analysis of the effectiveness of existing cyber security programs and cyber security controls. The CSAT documents the collected cyber security information and the results of their examination of the collected information.

3.1.5 Tabletop Reviews and Validation Testing

The CSAT conducts a tabletop review and validation activities.

Results of tabletop reviews and validation reviews are documented.

For each CDA/CDA group, the CSAT:

- Confirms the location;
- Confirms direct and indirect connectivity pathways;
- Confirms infrastructure interdependencies;
- Reviews any CDA assessment documentation;
- Reviews the defensive strategies;
- Reviews the defensive models;
- Confirms the implementation of plant-wide physical and cyber security policies and procedures that secure the CDAs from a cyber attack, including attack mitigation, and incident response and recovery;
- Confirms that staff members working with the CDAs are trained to a level of cyber security knowledge commensurate with their assigned responsibilities; and
- Identifies and documents the CDA cyber security exposures including specific attack/threat vectors to be assessed for mitigation using the method in Section 3.1.6.

The above activities are validated for CDAs through walk-downs. These walk-downs include:

- Performing, where practical, a physical inspection of the connections and configuration of CDAs, including tracing communication connections into and out of the CDA to termination points along communication pathways.
- Performing electronic validation when physical walk-down inspections are impractical to trace a communication pathway to its conclusion. When there is a risk of operational disruption, electronic validation tests are conducted during periods of scheduled outage. Where used, a justification of the adequacy of the electronic validation technique is documented.
- Examining the physical security established to protect CDAs and the CDA's communication pathways.
- Examining the configuration and assessing the effectiveness of cyber security controls (e.g., firewalls, intrusion detection systems, data diodes) along the communication pathways.
- Examining interdependencies with other CDA(s) and trust relationships between the CDA(s).
- Examining interdependencies with infrastructure support systems including electrical power, environmental controls, and fire suppression equipment which, if compromised, could adversely impact the proper functioning of CDAs.
- Resolving information and/or configuration discrepancies identified during the tabletop reviews, including the presence of undocumented and/or missing connections, and other cyber security-related irregularities associated with the CDA.

Information and/or configuration discrepancies identified during the tabletop reviews and walk-downs, including the presence of undocumented and/or missing connections, and other cyber security-related irregularities associated with the CDA are documented for remediation in the Corrective Action Program.

3.1.6 Mitigation of Vulnerabilities and Application of Cyber Security Controls

Defense-in-depth strategies are established by documenting and implementing the:

- Defensive strategy described in Section 4.3;
- Technical cyber security controls in Appendix D of NEI 08-09, Revision 7 consistent with the process described below; and
- Operational and Management cyber security controls in Appendix E of NEI 08-09, Revision 7 consistent with the process described below.

The CSAT utilizes the information gathered in Sections 3.1.3 through 3.1.5 to document how each of the technical cyber security controls were addressed for each CDA using the process described below. Other plant organizations may be used to implement the CSAT recommendations. For example, the Plant/Design Engineering group will perform requisite modifications to CDAs.

Cyber security controls are not applied if the control adversely impacts safety and important-to-safety, security or emergency preparedness functions, OR when alternate controls are implemented that mitigate the consequence(s) of the threat/attack vector associated with the control. Alternate controls are used to mitigate the lack of the security control for the CDA per the process described in this section.
For CDAs with multiple controls / countermeasures in place to mitigate the same threat / attack vectors, defense-in-depth is maintained so long as no single point of failure exists within the strategy that would adversely impact the CDA(s).

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. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 7.
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.

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.

3.1.7 Assessing Defense-in-Depth

The cyber security controls in this plan, in combination with the security controls prescribed by 10 CFR 73.55(b) may implement more than one barrier against exploitation of a cyber attack threat vector.

As noted at the beginning of Section 3, implementing Appendix D and E cyber security controls provides high-assurance of adequate protection of CDAs associated with SSEP functions, creating a substantive defense-in-depth cyber security program with significant layers of protection. This comprehensive approach to implementing technical, operational, and programmatic security controls creates a robust cyber defensive posture such that the degradation of a subset of security control(s) does not inherently reduce margin of adequate protection of the SSEP function.

In cases where there is degradation or failure of a specific cyber security control, margin may exist. Before making that determination, the impact of degradation or failure must be assessed to determine the effect(s) on defense-in-depth protections. The licensee must also assess the CDA, the relevant attack vectors, and the intent of the degraded cyber control in accordance with the process described in Section 3.1.6.

If protections still exist, such that the degradation or failure of the CDA controls would not result in a substantive increase of an adversary's ability to successfully exploit the threat / attack vector(s) that the control is intended to protect, then the effect(s) of the degradation or failure on defense-in-depth would be reduced. When a degradation or failure of a cyber security control is identified, it must be entered into the licensee's corrective action program for remediation.

3.2 RECORDS

Records of the assessment described in Section 3.1 of this Plan are maintained in accordance with approved procedures as described in Section 4.13 of this Plan.

4 ESTABLISHING, IMPLEMENTING, AND MAINTAINING THE CYBER SECURITY PROGRAM

This section establishes the programmatic elements necessary to maintain cyber security throughout the life cycle of CDAs. The elements of this section are implemented to maintain high assurance that CDAs associated with the SSEP functions are adequately protected from cyber attacks up to and including the DBT.

A life cycle approach is employed consistent with the controls described in Appendix E of NEI 08-09, Revision 7. This approach ensures that the cyber security controls established and implemented for CDAs are maintained to achieve the site's overall cyber security program objectives. For proposed new digital assets, or existing digital assets that are undergoing modification, the process described in Sections 10 and 11 of the Operational and Management controls of NEI 08-09, Revision 7, Appendix E are implemented.

Records are maintained in accordance with Section 4.13 of this Plan.

4.1 Incorporating The Cyber Security Program Into The Physical Protection Program

The Cyber Security Program, which is referenced in the Physical Security Plan, implements the Cyber Security Program requirements in accordance with 10 CFR 73.54(b)(3), 10 CFR 73.55(a)(1), and 10 CFR 73.55(c)(6). Cyber attacks are also considered during the development and identification of target sets as required by the Physical Security Program and 10 CFR 73.55(f)(2).

Revisions to this Plan are processed in accordance with procedures that implement the requirements of 10 CFR 50.54(p). Changes that are determined to decrease the effectiveness of this Plan are submitted to the NRC for approval as required by 10 CFR 50.90.

The Cyber Security Program is reviewed as a component of the Physical Security Program as required by 10 CFR 73.55(m).

4.2 Cyber Security Controls

The Technical, Operational and Management Cyber Security Controls described in Appendices D and E of NEI 08-09 Revision 7, are evaluated and dispositioned based on site specific conditions during the establishment of risk baselines, during on-going programs, and during oversight activities.

Cyber security controls are used to protect CDAs within the scope of the Rule. The cyber security controls are implemented utilizing the process described in Section 3.1.6 of this Plan.

Management controls, Operational controls, and Technical controls, in conjunction with Physical Security Plans, support the overall safety of nuclear material and reliability of plant operations. The Cyber Security Controls are utilized in site [Baseline Assessment, Configuration Management, Engineering Design Control, Training, Attack Mitigation and Incident Response, Record Retention and Handling, and Review] programs.

If a CDA cannot support the use of automated cyber security control mechanisms, non-automated cyber security control mechanisms or procedures are documented and utilized where necessary to maintain the desired level of protection.

Many security controls have actions that are required to be performed on specific frequencies. The frequency of a security control is met if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action. This extension facilitates scheduling and considers plant operating conditions that may not be suitable for conducting the security control action (e.g., transient conditions, other ongoing surveillance or maintenance activities). These provisions are not intended to be used repeatedly merely as an operational convenience to extend frequencies beyond those specified.

4.3 DEFENSE-IN-DEPTH PROTECTIVE STRATEGIES

Defense-in-depth protective strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyber attacks on CDAs. The defensive strategy describes the defensive security architecture, identifies the protective controls associated within each security level, implements cyber security controls in accordance with Section 3.1 of this Plan, employs the Defense-in-Depth measures described in NEI 08-09, Appendix E, Section 6, and maintains the cyber security program in accordance within Section 4 of this Plan.

The defensive architecture has been implemented, documented, and is maintained to protect CDAs that have similar cyber risks from other CDAs, systems or equipment by establishing the logical and physical boundaries to control the data transfer between boundaries.

This defensive architecture provides for cyber security defensive levels separated by security boundaries devices, such as firewalls and diodes, at which digital communications are monitored and restricted. Systems requiring the greatest degree of security are located within the greatest number and strength of boundaries. The criteria below are utilized in the defensive architecture.

[
Insert site-specific Defensive Architecture description that answers the following three questions:

1. In what level or levels are safety and security CDAs located?
2. What are the boundaries, and what are the data flow rules between defensive levels?
3. How are the data flow rules enforced? For example, if a deterministic boundary device is used, the description can be brief (e.g., data flow is enforced between levels 3 and 4 using a data diode). However, if a non-deterministic boundary device is used (e.g., a firewall), the plan needs to include the criteria that the device will apply to enforce the data flow rule (e.g., Section 6 of NEI 08-09, Revision 7, Appendix E non-deterministic data flow criteria).

Two hypothetical examples are provided below to illustrate the level of detail sufficient for this section:

Example 1:

The site defensive model implements all of the following:

- The defensive model consists of 4 layers, with layer 4 having the greatest level of protection.
- Safety CDAs are in Level 4.
- Security CDAs are air gapped or are located behind a unidirectional deterministic boundary device with the exception of communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications that require bi-directional communication to meet regulatory and plan requirements.

- The boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above Level 3. Information flows between Level 3 and 4 are restricted through the use of a firewall and network-based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 7, Appendix D, Section 1.4 and the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 7, Appendix E, Section 6.

Example 2:

The site defensive model implements all of the following:

- The defensive model consists of 4 layers, with layer 4 having the greatest level of protection.
- Safety CDAs are in Level 4.
- Safety CDAs are isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air-gaps).
- Security CDAs are air gapped or are located behind a unidirectional deterministic boundary device with the exception of communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications that require bi-directional communication to meet regulatory and plan requirements.
- Information flows between Security CDAs in one level and Security CDAs in another level are restricted through the use of a firewall and network-based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 7, Appendix D, Section 1.4.

]

For this defensive architecture to be effective in protecting CDAs from cyber attacks the above characteristics are consistently applied, along with the technical, management, and operational security controls discussed in Appendices D and E of NEI 08-09, Revision 7.

The cyber security defensive model is enhanced by physical and administrative cyber security controls implemented by the Physical Security Program. Physical barriers such as locked doors, locked cabinets, and/or locating CDAs in the protected area or vital area are also used to mitigate risk.

4.4 Ongoing Monitoring And Assessment

Ongoing monitoring of cyber security controls used to support CDAs is implemented consistent with Appendix E of NEI 08-09, Revision 7. Automated support tools are also used, where available, to accomplish near real-time risk management for CDAs. The ongoing monitoring program includes:

- Configuration management of CDAs;

- Cyber security impact analyses of changes to the CDAs or their environment(s) to ensure that implemented cyber security controls are performing their functions effectively;
- Ongoing assessments to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle of the CDA;
- Verification that rogue assets are not connected to the network infrastructure;
- Ongoing assessments of the need for and effectiveness of the cyber security controls identified in Appendices D and E of NEI 08-09, Revision 7; and
- Periodic cyber security program review to evaluate and improve the effectiveness of the Program.

This element of the Program is mutually supportive of the activities conducted to monitor configuration changes of CDAs.

4.4.1 Configuration Management and Change Control

The configuration management controls described in Appendix E of NEI 08-09, Revision 7, have been implemented as described in Section 3.1.6, and implementation has been documented. A configuration management approach is implemented to update and maintain cyber security controls for CDAs in order to ensure that the cyber security program objectives remain satisfied. Modifications to CDAs are evaluated before implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained. A record of changes made to the configuration of CDAs is maintained.

CDA cyber security and configuration management documentation is updated or created using the site configuration management program or other configuration management procedure or process. This documentation includes the bases for not implementing one or more of the technical cyber security controls specified in Appendix D of NEI 08-09, Revision 7.

During the operation and maintenance phases of the CDA life cycle, changes to CDAs are made using [Design Control and Configuration Management procedures], so that additional cyber security risk is not introduced into the system. The process ensures that the controls specified in Appendices D and E of NEI 08-09, Revision 7, have been implemented in a manner consistent with this Plan and implementing procedures.

During the retirement phase, the [Design Control and Configuration Management procedures] address SSEP functions.

4.4.2 Cyber Security Impact Analysis of Changes and Environment

A cyber security impact analysis is performed prior to making a design or configuration change to a CDA, or when changes to the environment occur, consistent with the process described in Section 4 of the Operational and Management Controls of Appendix E to NEI 08-09, Revision 7, to manage risks introduced by the changes.

Interdependencies of other CDAs or support systems are evaluated, documented, and incorporated into the cyber security impact analysis. The steps for conducting the tabletop review described in Section 3.1.5 are performed.

These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of CDAs and systems that can affect SSEP functions. Cyber security related issues identified during the change management process are addressed within the change management process and therefore are not handled by the Corrective Action Program. Adverse conditions identified after the modification is implemented are entered into the site Corrective Action Program.

Risks to SSEP functions, CDAs and CSs are managed through ongoing evaluation of threats and vulnerabilities and by addressing threat and attack vectors associated with the cyber security controls provided in Appendices D and E of NEI 08-09, Revision 7, during the various phases of the life cycle. Additionally, procedures are developed for screening, evaluating, mitigating and dispositioning threat and vulnerability notifications received from credible sources. Dispositioning includes implementation, as necessary, of cyber security controls to mitigate newly reported or discovered vulnerabilities and threats.

4.4.3 Ongoing Assessment of Cyber Security Controls

Ongoing assessments are performed to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle. The assessment process verifies the status of these cyber security controls [at least every 24 months] or in accordance with the specific requirements for utilized cyber security controls as described in Appendices D and E of NEI 08-09, Revision 7, whichever is more frequent.

4.4.3.1 Effectiveness Analysis

The effectiveness and efficiency of the Cyber Security Program and the cyber security controls in Appendices D and E of NEI 08-09, Revision 7, are monitored to confirm that the cyber security controls are implemented correctly, operating as intended, and continuing to provide high assurance that CDAs are protected against cyber attacks up-to and including the DBT. Reviews of the cyber security program and controls include, but are not limited to, periodic audits as a component of the physical security program and feedback from NRC inspections and other program assessments.

The effectiveness analysis should provide information for evaluating corrective actions implemented pertaining to the cybersecurity program and the enrollment of newly installed plant equipment in the cybersecurity program. Key information in these areas should support the ongoing analysis regarding the effectiveness of the implemented program. The effectiveness analysis should also do the following:

- Provide insight for improving performance of the Cyber Security Program;
- Assist in determining the effectiveness of cyber security controls in Appendices D and E of NEI 08-09, Revision 7;

- Facilitate corrective action prioritization; and
- Provide reviews for both programmatic activities and data obtained from automated monitoring in order to present an overall picture of program health.

The effectiveness of these cyber security controls is verified when applied, and [at least every 24 months] or in accordance with the specific requirements for employed cyber security controls as described in Appendices D and E of NEI 08-09, Revision 7, whichever is more frequent. Documents of maintenance and repairs on CDA components are reviewed to ensure that CDAs which perform cyber security functions are maintained according to recommendations provided by the manufacturer or as determined by site-specific procedures.

Adverse conditions identified during effectiveness evaluations are entered in the site Corrective Action Program.

4.4.3.2 Vulnerability Assessments and Scans

Vulnerability assessments or electronic vulnerability scanning of CDAs are performed as described in Appendix E, 12, "Evaluate and Manage Cyber Risk," when new vulnerabilities that could affect the cyber security posture of CDAs are identified.

When new vulnerabilities are discovered, they are evaluated against the threat vectors associated with the vulnerability. Vulnerabilities that pose a risk to SSEP functions are mitigated when the evaluation concludes remediation is required to maintain adequate defense-in-depth. Applicable vulnerability reviews are kept as a record. Vulnerabilities requiring mitigation are documented in the Corrective Action Program (CAP).

Prior to performing vulnerability scans, risk of operational disruption must be considered. The assessment and scanning process must not adversely SSEP functions. If this could occur, CDAs are removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. Scans should be conducted during scheduled outage periods. Development or test beds or vendor-maintained environments may be used to perform vulnerability scans.

4.5 Addition And Modification Of Digital Assets

The approach for assessing new/modified CDAs is to use the assessment process described in Section 3.1 of this Plan.

[Programs, Procedures, Processes] have been established, implemented, and maintained to control life cycle phase activity cyber security controls for CDAs. These [programs, procedures, processes] ensure that modifications to a CDA within the scope of 10 CFR 73.54 are evaluated before implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained and that acquired CDAs have cyber security requirements developed to achieve the site's cyber security program objectives.

Records are maintained in accordance with Section 4.13 of this Plan.

4.6 ATTACK MITIGATION AND INCIDENT RESPONSE

The Program ensures that the Safety, Security, and Emergency Preparedness functions of digital assets within the scope of the Rule (CDAs) are not adversely impacted due to cyber attacks. Appendix E of NEI 08-09, Revision 7, includes the following topics pertaining to attack mitigation and incident response:

- Incident Response Policy and Procedures
- Incident Response Training
- Incident Response Testing and Drills
- Incident Handling
- Incident Monitoring
- Incident Response Assistance

[Policies, Procedures, Programs] document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs that may be susceptible to cyber attacks which exploit system vulnerabilities. Cyber security controls employed counteract threats. [Policies, Procedures, Programs] document the methods to handle digital-related adverse conditions.

Digital-related adverse conditions are entered into the site Corrective Action Program for resolution. If the condition affects a CDA, the condition is evaluated to determine if there is reason to believe that the condition is the result of a cyber attack. If there is reason to believe the condition is the result of a cyber attack, the event is reported to the NRC in accordance with 10 CFR 73.77.

Identification, detection, and response to cyber attacks are directed by site procedures for cyber security and other procedures that govern response to plant events. When there is reasonable suspicion of a cyber attack, response instructions direct notification to the [Shift Superintendent Operations, Site Security Superintendent, Manager Nuclear Information Technology, activation of Cyber Security Incident Response Team]. Response instructions direct other emergency response actions, if warranted.

Cyber security attack containment activities are directed by site procedures. These measures include but are not limited to:

- Assist in determining the CDA's operability or functionality;
- Isolate the affected CDA with approval by [Shift Superintendent Operations], if possible; and
- Verify surrounding networks and support systems are not contaminated.

Eradication activities identify the attack and the compromised pathway, patch or clean the CDA, or replace the CDA using disaster recovery procedures. Measures necessary to mitigate the consequences of cyber attacks are as directed by site governing procedures.

Recovery activities include but are not limited to functional recovery test, cyber security function and requirements tests, restoration to operational state, verification of operability or functionality, and return to service. Systems, networks, and/or equipment affected by cyber attacks are restored and returned to operation as directed by site procedures. Post incident analysis is conducted in accordance with site Corrective Action Program procedures.

4.7 CYBER SECURITY CONTINGENCY PLAN

A Cyber Security Contingency Plan protects CDAs from adverse impacts from cyber attack. Refer to Appendix E of NEI 08-09, Revision 7, for additional Cyber Security Contingency Plan cyber security controls.

The contingency planning policy is developed, disseminated, periodically reviewed and updated. The contingency planning policy provides the following:

a. A formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the policy and associated contingency planning controls.

The Cyber Security Contingency Plan includes:

- Required response to events or conditions of varying duration and severity that would activate the recovery plan;
- Procedures for operating the CDAs in manual mode with external electronic communications connections severed until secure conditions can be restored;
- Roles and responsibilities of responders;
- Processes and procedures for the backup and secure storage of information;
- Complete and up-to-date logical diagrams depicting network connectivity;
- Current configuration information for components;
- Personnel list (according to title and/or function) for authorized physical and cyber access to the CDA;
- Communication procedure and list of personnel (according to title and/or function) to contact in the case of an emergency; and
- Documented requirements for the replacement of components.

4.8 CYBER SECURITY TRAINING AND AWARENESS

The Program establishes the training requirements necessary for licensee personnel and contractors to perform their assigned duties and responsibilities in implementing the requirements of the Program.

Individuals are trained to a level of cyber security knowledge commensurate with their assigned responsibilities in order to provide high assurance that individuals are able to perform their job

functions. Refer to Appendix E of NEI 08-09, Revision 7, which describes the Cyber Security Controls required for the following levels of training:

- Awareness Training
- Technical Training
- Specialized Cyber Security Training

Specific topics included within the Cyber Security Training and Awareness program may be modified, added or deleted (1) in response to feedback from personnel and contractors who have taken the training or (2) as a result of discussions with cyber security groups and associations.

4.9 EVALUATE AND MANAGE CYBER RISK

Cyber risk is evaluated and managed utilizing site programs and procedures.

4.9.1 Threat and Vulnerability Management

Cyber risks are managed through evaluation of threats and vulnerabilities to computer and control systems during the life cycle phases as documented in the [Engineering Design Control, Configuration Management, Software Quality Assurance, Operating Experience (OE) and Corrective Action Program (CAP)] processes. The Program establishes [in procedures or other plant documents] how responses to threat notifications and vulnerabilities against a CDA received from a credible source are screened, evaluated and dispositioned.

4.9.2 Risk Mitigation

Protection and mitigation of cyber risk are achieved by applying cyber security controls to the CDAs within the scope of the Rule. Detailed information on how these requirements are implemented to achieve high assurance objectives of cyber security controls specified in this Plan is available on site for the NRC's inspections and audit.

4.9.3 Operational Experience

[Policies, Procedures, Programs] establish how the operational experiences related to cyber security are screened to determine applicability, evaluated to determine significance, and dispositioned in an [operational experience program]. Any condition determined to be adverse as a result of the evaluation of operational experiences, is dispositioned in the Corrective Action Program.

4.9.4 Corrective Action Program

[Policies, Procedures, Programs] establish the criteria for adverse conditions and the requirements for corrective action. Adverse impact resulting from a cyber security condition is evaluated, tracked and dispositioned in accordance with the site Corrective Action Program.

4.10 Policies And Implementing Procedures

Policies and implementing procedures are developed to meet the implemented cyber security control's objectives provided in Appendices D and E of NEI 08-09, Revision 7. The program policies and implementing procedures are documented, developed, reviewed, approved, issued, used, and revised as described in Section 4 of this Plan. Program policies and implementing procedures establish that personnel responsible for the management and implementation of the program report [directly or indirectly] to senior nuclear management. Senior nuclear management is [Chief Nuclear Officer, Chief Nuclear Operations Officer, Vice President of Nuclear Operations, Vice-President] who is accountable for nuclear plant(s) operation.

Implementing procedures establish responsibilities for the positions documented in Section 4.11.

4.11 Roles And Responsibilities

Roles and responsibilities are implemented with site procedures to preclude conflict during both normal and emergency conditions. The following Roles are created and staffed with qualified and experienced personnel. Authorized contracted resources possessing the skill set identified below for their designated role may be used. Implementing procedures establish responsibilities for the following:

Cyber Security Program Sponsor

- Member of Senior [Site/Licensee] Management;
- Overall responsibility and accountability for the cyber security program;
- Provide resources required for the development, implementation and sustenance of the cyber security program;
- Accountable to meet the needs of the site and receives support and compliance; and
- Ensure that resources are available to develop and implement the Program.

Cyber Security Program Manager

- The single point of contact accountable for any issues related to [Site/Licensee] cyber security;
- Responsible for oversight and assuring periodic assessments are performed in accordance with Section 4;
- Provides oversight of the plant cyber security operations;
- Functions as a single point of contact for issues related to cyber security;
- Provides oversight and direction on issues regarding nuclear plant cyber security;
- Initiates and coordinates Cyber Security Incident Response Team (CSIRT) functions as required;
- Coordinates with NRC, DHS, DOE, and FBI as required during cyber security events;
- Oversees and approves the development and implementation of a Cyber Security Plan;
- Ensures and approves the development and operation of the cyber security education, awareness, and training program; and
- Oversees and approves the development and implementation of cyber security policies and procedures.

Cyber Security Specialists

- Protect CDAs from cyber threat;
- Understand the cyber security implications surrounding the overall architecture of plant networks, operating systems, hardware platforms, plant-specific applications, and the services and protocols upon which those applications rely;
- Perform cyber security assessments of CDAs;
- Conduct cyber security audits, network scans, and penetration tests against CDAs as necessary;
- Conduct cyber security investigations involving compromise of CDAs;
- Preserve evidence collected during cyber security investigations to prevent loss of evidentiary value;
- Maintain expert skill and knowledge level in the area of cyber security; and
- Receive specialized cyber security training described in Section 4.8.

Cyber Security Incident Response Team (CSIRT)

- Initiates in accordance with the Incident Response Plan;
- Initiates emergency action when required to safeguard CDAs from cyber security compromise and to assist with the eventual recovery of compromised systems;
- Contains and mitigates incidents involving critical and other support systems;
- Restores compromised CDAs; and
- Responds to a cyber attack and performs the activities described in Section 4.6. Responsibilities are designated in site [incident/event response] procedures. Ancillary CSIRT staff includes organizations and individuals who operate, maintain, or design critical systems. CSIRT support staff is comprised of organizations and individuals as needed for specific specialized knowledge.

Others

Operators, engineers, technicians, and users perform their assigned duties in accordance with the requirements of the Program.

4.12 CYBER SECURITY PROGRAM REVIEW

The Cyber Security Program established the necessary measures and governing procedures to implement reviews of applicable program elements in accordance with the requirements of 10 CFR 73.55(m). Security Controls are elements of the Security Program and are reviewed consistent with the following requirements of 10 CFR 73.55(m).

(1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:

(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.
(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.

(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.

(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program.

4.13 Document Control And Records Retention And Handling

[Site/Licensee] has established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work.

The following will be retained as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission:

- Records of the assessment described in Section 3.1 of this Plan;
- Records that are generated in the Establishment, Implementation, and Maintenance of the Cyber Security Program;
- Records of Addition and Modification of Digital Assets; and
- Records and supporting technical documentation required to satisfy the requirements of the Rule.

CDA audit records will be retained for no less than 12 months. CDA auditing capabilities are configured in accordance with section 3.1.6 of this plan.

Where a central logging server is employed, the audit records received will be retained for no less than 12 months.

The following audit data will be retained:
- Audit data described in Appendix D, 2.3, “Content of audit records”

- Audit data that support Appendix E, “Defense-in-Depth” security control will be retained to provide support for after-the-fact investigations of security attacks and satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55.

Audit (digital and non-digital) data include:
- Operating system logs
- Service and application logs
- Network device logs

For the purposes of this Plan, audit data is not required to be maintained under the QA Records Program.

Individual Cyber Security Training Records will be documented and maintained for 3 years.

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX B: GLOSSARY

The glossary in NEI 08-09 defines only those terms that are specific to their usage in NEI 08-09. Other terms should be referenced in the following order of preference.

1. Specific terms defined in Rules.
2. NEI Scope of Systems white paper for clarification of 73.54(a)(1) systems.
3. NIST IR 7298 Glossary of Key Information Security Terms.
4. RG 5.71 Rev.1, February 2023
5. Webster's dictionary

Access Control
The control of entry or use, to all or part, of any physical, functional, or logical component of a CDA.

Adversary
Individual, group or organization that has adversely impacted or is attempting to adversely impact a CDA.

Adverse Impact
A direct deleterious effect on a CDA (e.g., loss or impairment of SSEP function, reduction in reliability, reduction in the ability to detect, delay, assess or respond to malevolent activities, reduction of ability to call for or communicate with offsite assistance, and the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency). In the case where the direct or indirect compromise of a support system causes a safety-related, important-to-safety, security or emergency preparedness system or support system to actuate or "fail safe" and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds), this is not considered to be an adverse impact in the context of 10 CFR 73.54(a).

ALNOTS
An Institute of Nuclear Power Operations (INPO) hosted software tool that compares a Licensee's grouped CDA inventory by manufacture and model number against publicly-known vulnerabilities documented in the US-CERT, ICS-CERT and National Vulnerability Database (NVD) web site resources. ALNOTS identifies vulnerabilities applicable to a Licensee's grouped CDA inventory that require further assessment and potential mitigation or remediation.

CVSS Attack Vector
For the purpose of vulnerability management assessment, this metric reflects the context by which vulnerability exploitation is possible. The full description may be found at First.Org. Values are Network, Adjacent, Local, and Physical. This term is sometimes referred to as "attack pathway".

Attempts to Cause
Efforts to accomplish a threat, even though it has not occurred or has not been completed because it was interrupted, stopped before completion, or may occur in more than two hours, as established through reliable and substantive information.

Balance of Plant SSC (BOP)
Systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system.

Commercial Off-The-Shelf (COTS) Software
Commercial devices or software (that is shipped and received with normal and expected vendor shipping packaging such as shrink-wrap, tamper seal or other recognizable packaging and marking) that is available from multiple sources developed to run unmodified as delivered by the original developer. This would include such products as commercially available operating systems (i.e. MS Windows, Linux, OSX, TXS, etc.) general purpose application software, (i.e. MS Office, Corel, Open Office, SQL Server, etc.) and open source products whose builds can be verified and are obtained from known trusted sources. Firmware such as that for a BIOS, field upgradable commercial sensor (i.e. Pressure Transmitters, Flow Sensors, Level Sensors, etc.), or other off the shelf upgradable hardware (i.e. Hard Drives, Video Cards, DVD Drives, Embedded OS, etc.) would be considered COTS.

Compromise
Loss of confidentiality, integrity, or availability of data or system function.

Credible
Information received from a source determined to be reliable (e.g. law enforcement, government agency, etc.) or has been verified to be true. A threat can be verified to be true or considered CREDIBLE when: Physical evidence supporting the threat exists, Information independent from the actual threat message exists that supports the threat, **or** a specific known group or organization claims responsibility for the threat.

Critical Digital Asset (CDA)
A digital computer, communication system, or network that is:
- a component of a critical system (this includes assets that perform SSEP functions; provide support to, protect, or provide a pathway to Critical Systems); or
- a support system asset whose failure or compromise as the result of a cyber attack would result in an adverse impact to a SSEP Function.

Critical System (CS)
A system that is associated with or provides safety-related functions; important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; or support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Custom Software
Any non-general purpose software product that has been customized to run on a hardware platform developed using any combination of commercial software and original coding to create an application or operating system that is purpose driven. This includes custom firmware designed to program or map hardware for a specific purpose (PLC, FPGA, EPROM and other programmable logic devices) and code that has been independently developed to enhance COTS software (portable code, macros, scripting, Visual Basic for Scripting, etc.)

Cyber Attack
Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a SSEP function.

[Note: Derived from the following sources: 10CFR 73.71(b); 10CFR 73 Appendix G; DG-5019, 10CFR 73.55(f); 72 FR 12723, 12724]

Cyber Incident
A digital-related adverse condition.

Integrity
Quality of a system reflecting the logical correctness and reliability of the operation of the system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Additionally, integrity includes protection against unauthorized modification or destruction of information.

Interruption of Normal Operation
A departure from normal operations or conditions that, if accomplished, would result in a challenge to the facility's safety, security, or emergency response systems. This may also include an event that causes a significant redistribution of security, safety, or emergency response resources. This could include intentional tampering with systems or equipment that is normally in a standby mode, but would need to operate if called upon in an abnormal or emergency situation. Section 236 of the AEA (42 U.S.C. Section 2284) treats as sabotage the knowing interruption of normal operation of any such facility through the unauthorized use of, or tampering with, the machinery, components, or controls of any such facility, or attempting or conspiring to carry out such an act.

Malware
Malicious software designed to infiltrate or damage a CDA, CS or protected network without licensee consent. Malware includes computer viruses, worms, Trojan horses, Root kits, spyware, adware and other potentially unwanted programs.

Mitigation
Corrective actions that address the attack vector(s) associated with a cyber security vulnerability and reduce the likelihood of exploit by implementing one or more alternate security controls that improve CDA security control protections.

Mobile Code
Programs or parts of programs obtained from remote control systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Patch
A fix for a CDA or software program where the actual binary executable and related files are modified. **Portable Media and Mobile Devices** (PMMD)
Any portable cartridge / disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives/devices that contain nonvolatile memory) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, test equipment, tablets, personal digital assistants, cellular telephones, digital cameras, audio recording devices).

Portable Media and Mobile Devices (PMMD)
Any portable cartridge / disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives/devices that contain nonvolatile memory) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, test equipment, tablets, personal digital assistants, cellular telephones, digital cameras, audio recording devices).

Recovery
Steps taken to restore a system, function, or device to its original state of operation following a catastrophic or partial loss of functionality or when an original state of operation is challenged by either an event (such as a cyber attack) or anomaly (behavior not expected from normal operation).

Remediation
Installation of a physical security control or software patch, fix or configuration change that addresses the known cyber security vulnerability.

Social Engineering Techniques
Attempts by unauthorized individuals to gain physical or electronic (e.g., password) access to systems via impersonation of authorized functions or personnel.

Tampering (Cyber)
Altering, disabling, or damaging digital computer and communications systems and networks or cyber security controls for improper purposes or in an improper manner.

Critical Group
Any individual who performs job functions that are critical to the safe and secure operation of the licensee's facility. This individual includes:

1) anyone who has been granted unescorted access or certified with unescorted access authorization
   AND

2) performs one or more of the following job functions:
a. has extensive knowledge of facility defensive strategies or designs and/or implements the plant's defense strategies
b. can grant an individual unescorted access or to certify an individual unescorted access authorization
c. is assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices)
d. has the combination of electronic access and the administrative control (e.g., "system administrator rights") to alter one or more security controls associated with one or more critical digital assets (CDAs)
e. has extensive knowledge of the site-specific cyber defensive strategy.

"Extensive knowledge" is defined as having (1) knowledge of the cybersecurity controls in place for a CDA, or (2) knowledge of how the configuration of a CDA or the cybersecurity controls can be modified in a manner that could result in an adverse impact to safety or important-to-safety, security, or emergency preparedness (SSEP) functions.

Individuals performing the following functions should be included:

- site cybersecurity supervisors
- site cybersecurity manager
- site cybersecurity training manager
- corporate cybersecurity manager

"Administrative control" is defined as the electronic access and rights to independently change either the configuration of a CDA or the cybersecurity controls in place for a CDA, in a manner that could result in an adverse impact to SSEP functions.

Individuals performing the following functions should be included, as applicable:

- cybersecurity engineers and administrator,
- information technology personnel who are responsible for authorizing access to CDAs
- CDA system administrators
- personnel who can independently change the configuration of CDAs or can alter security controls

f. Licensed reactor operators
g. Non–licensed operators. Non-licensed operators include those individuals responsible for the operation of plant systems and components, as directed by a reactor operator or senior reactor operator. Non-licensed operators also monitor plant instrumentation and equipment and principally perform their duties outside the control room.

SRM SECY 16-0073, "HIGH ASSURANCE is equivalent to "REASONABLE ASSURANCE"

In implementing the NRC's regulatory program, either in developing new regulations, inspecting licensee compliance with regulations, or executing the FOF program, the staff should be mindful that the concept of "high assurance" of adequate protection found in our security regulations is equivalent to "reasonable assurance" when it comes to determining what level of regulation is appropriate. The NRC should not be applying a "zero risk" mentality to security any more than we should be doing so with respect to safety. The staff should operate

under this paradigm and eliminate ambiguity on this point in its guidance documents or other internal directives, instructions, or training materials, to the extent such ambiguity exists.

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX C

[Deleted]

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX D: TECHNICAL CYBER SECURITY CONTROLS

The Technical Cyber Security Controls in this appendix represent methods for the mitigation of risks to digital systems. When implementing cyber security controls, discretion may be taken with the means by which the control is implemented. When a control or aspects of a control are not implemented, an analysis is performed to ensure that the risk is effectively mitigated. A security control is considered to be applied when there is high assurance that the CDA is adequately protected from the risk considered by the security control. Section 3.1.6 of NEI 08-09, Revision 7, Appendix A, provides a multi-step process for the analysis and documentation of the application of cyber security controls.

Security Controls are elements of the Security Program and are reviewed consistent with the requirements of 10 CFR 73.55(m).

1 ACCESS CONTROLS

1.1 ACCESS CONTROL POLICY AND PROCEDURES

A formal, documented, critical digital asset (CDA) access control policy is developed, disseminated, and reviewed in accordance with 10 CFR 73.55(m), and updated. This access control program addresses purpose, scope, roles, responsibilities, management commitment, and internal coordination; and formal, documented procedures that facilitate the implementation of the access control policy and associated access security controls.

The objective of the access control policy is to provide high assurance that only authorized individuals and/or processes acting on their behalf can access CDAs and perform authorized activities. The access control policy addresses the following system-specific requirements: Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, System Use Notification, Previous Login Notification, Session Lock, Session Termination, Supervision and Review/Access Control, Permitted Actions Without Identification or Authentication, Automated Marking, Automated Labeling, Remote Access, Wireless Access Restrictions, and Access Control for Portal and Mobile Devices and Use of External CDAs.

The access control policy addresses:

- Access control rights (i.e., which individuals and processes can access what resources) and access control privileges (i.e., what these individuals and processes can do with the resources accessed);
- Management of CDAs (i.e., accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts);
- Protection of password/key databases to prevent unauthorized access to master user/password list(s);
- Auditing of CDAs every 12 months, or upon changes in critical group personnel or major changes in system configurations or functionality; and
- Separation of duties (i.e., through assigned access authorizations).

1.2 ACCOUNT MANAGEMENT

This Technical cyber security control:

- Manages and documents CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts.
- Reviews CDA accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on temporary granted CDA accounts at least every 31 days.
- Licensee policies/procedures shall not allow temporary, guest, and emergency accounts unless their use is documented.
- Accounts on CDAs (Group or individual) shall only be authorized/terminated through station policies/procedures.
- Requiring access rights to be job function based.
- Any unauthorized accounts identified through an audit on a CDA will be documented in CAP for resolution.

For CDAs that do not utilize Centralized Account Management

- CDAs will use common role based group accounts to the extent possible. (Admin, User, Maintenance)
- Accounts will be used to enforce least privilege
- As a minimum, Accounts will be reviewed during maintenance/design activities where root/privileged level access is required.
- If individuals are granted unique access rights, then conduct reviews as individual's job function changes to ensure that rights remain limited to the individual's job function.

For CDAs that use utilize Centralized Account Management

- Accounts will be reviewed every 31 days.
- Conduct reviews when as individual's job function changes to ensure that rights remain to the individual's job function.

1.3 ACCESS ENFORCEMENT

This Technical cyber security control:

- Enforces assigned authorizations for controlling access to CDAs in accordance with established policies and procedures.
- Assigns user rights and privileges on the CDA consistent with the user authorizations.
- Defines and documents privileged functions and security-relevant information for the CDAs.
- Authorizes personnel access to privileged functions and security-relevant information consistent with established policies and procedures.
- Restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to authorized personnel (e.g., security administrators).
- Defines and documents privileged functions for CDAs.
- Requires dual authorization for critical privileged functions and to create any privileged access for users.

- Ensures and documents that access enforcement mechanisms do not adversely impact the operational performance of CDAs and employs alternate compensating security controls when access enforcement cannot be used.

1.4 INFORMATION FLOW ENFORCEMENT

This Technical cyber security control:

- Enforces and documents assigned authorizations for controlling the flow of information, in near-real time, within CDAs and between interconnected systems in accordance with the established defensive strategy.
- Maintains documentation that demonstrates the analysis and addressing of permissible and impermissible flow of information between CDAs, security boundary devices and boundaries and the required level of authorization to allow information flow as defined in the defensive strategy.
- Implements and documents information flow control enforcement using protected processing level as a basis for flow control decisions.
- Implements near-real time capabilities to detect, deter, prevent, and respond to illegal or unauthorized information flows.
- Prevents encrypted data from bypassing content-checking mechanisms.
- Implements one-way data flows using hardware mechanisms, implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.
- Implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.
- Configures CDAs such that user credentials are not transmitted in clear text, and documents this requirement in the access control policy.

1.5 SEPARATION OF FUNCTIONS

This Technical cyber security control:

- Establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest, and ensure independence in the responsibilities and functions of individuals.
- Enforces separation of CDA functions through assigned access authorizations,
- Implements alternative controls and documents the justification for alternative controls/countermeasures for increased auditing where a CDA cannot support the differentiation of roles and where a single individual must perform all roles within the CDA.
- Restricts security functions to the least amount of users necessary to ensure the security of CDAs.

1.6 LEAST PRIVILEGE

This Technical cyber security control:

- Assigns the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.
- Configures CDAs to enforce the most restrictive set of rights/privileges or access needed by users.
- Implements alternative controls and documents the justification for alternative controls/countermeasures for increased auditing where a CDA cannot support the differentiation of privileges within the CDA and where an individual must perform all roles within the CDA.

1.7 UNSUCCESSFUL LOGIN ATTEMPTS

This Technical cyber security control:

- Implements security controls to limit the number of invalid access attempts by a user and documented this requirement in the access control policy. The number of failed user login attempts per specified time period may vary by CDA. For example, greater than three (3) invalid attempts within a one (1) hour time period automatically locks out the account. The system enforces the lock out mode automatically.
- Ensures that accounts can only be unlocked by authorized individuals who are not the locked out user when the maximum number of unsuccessful login attempts has been exceeded, and documents this requirement in the access control policy. Alternatively, use of other verification techniques or mechanisms which incorporate identity challenges may be used.
- Documents the justification and details for alternative controls/countermeasures where a CDA cannot support account/node locking or delayed login attempts where CDAs do not support centralized logging:
    - Alternative controls/countermeasures are employed including: 24x7 monitoring, located in a Vital Area, located within a Locked Cabinet, or other physical control.
- Where a CDA cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, alternative controls/countermeasures are employed to include:
    - Real time logging and recording of unsuccessful login attempts.
    - Real time alerting of designated personnel with the security expertise for the CDA through alarms when the number of defined consecutive invalid access attempts is exceeded.

1.8 SYSTEM USE NOTIFICATION

This Technical cyber security control:

- Where the design of the CDA supports the use of System Use Notification message and implementation does not have an adverse impact on the SSEP function:
    - Displays a “System Use Notification” message before granting system access informing potential users:
    - That the user is accessing a restricted system.
    - That system usage may be monitored, recorded, and subject to audit.

  - That unauthorized use of CDAs is prohibited and subject to criminal and civil penalties, and
  - That the use of CDAs indicates consent to monitoring and recording.
- Ensures that CDA "System Use Notification" message provides privacy and security notices.
- Approves CDA "System Use Notification" message before its use.
- Ensures that CDA "System Use Notification" message remains on the screen until the user takes explicit actions to log on to the CDA.
- Installs physical notices at a central location to inform plant personnel of the potential consequences of unauthorized access to CDAs where System Use Notifications are not provided on the CDA.

1.9 PREVIOUS LOGON NOTIFICATION

DELETED

1.10 SESSION LOCK

CDAs are configured to:

- Initiate a session lock within 30 minutes of inactivity.
- Provide the capability for users to initiate session lock mechanisms.
- Maintain the session lock on a CDA until the user reestablishes access using identification and authentication procedures.
- Implement alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support session locks and implements the following:
  - Physically restricts access to the CDA,
  - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
  - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - Ensures that individuals who have access to the CDA are qualified, and
  - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

1.11 SUPERVISION AND REVIEW—ACCESS CONTROL

DELETED

1.12 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

This Technical cyber security control:

- Identifies and documents specific user actions that can be performed on CDAs during normal and emergency conditions without identification or authentication.
- Permits actions to be performed without identification and authentication to the extent necessary to accomplish mission objectives, without adversely affecting safety, security, and emergency preparedness functions.

1.13 AUTOMATED MARKING

This Technical cyber security control:

- Identifies and implements standard naming conventions for identification of special dissemination, handling, or distribution instructions in compliance with 10 CFR 2.390 and 10 CFR 73.21.
- Ensures CDAs are configured to mark hard and soft copy output using standard naming conventions to identify any special dissemination, handling, or distribution instructions (e.g., SRI information or SGI information).

1.14 AUTOMATED LABELING

DELETED

1.15 NETWORK ACCESS CONTROL

This Technical cyber security control establishes mitigation techniques to secure CDAs through MAC address locking, physical or electrical isolation, static tables, encryption, and/or monitoring are employed and documented.

1.16 "OPEN/INSECURE" PROTOCOL RESTRICTIONS

This Technical cyber security control:
If a protocol lacks security controls to protect networks and bus communications from unauthorized access, take the following additional precautions:

- Prohibits the protocols from initiating commands except within the same boundary.
- Prohibits these protocols from initiating commands that could change the state of the CDA from a more secured posture to a less secured posture.

1.17 WIRELESS ACCESS RESTRICTIONS

This Technical cyber security control:

- Restricts wireless devices to access through a boundary security control device and treats wireless connections as outside of the boundary.
- The use of wireless communications for the control of CDAs associated with SR and ITS functions is prohibited.

  [Note: "associated with" does not preclude the use of wireless technology for the use of monitoring nor data collection. The prohibition is directed at the use of wireless technology for manipulation (i.e. control) of the system safety functions. The use of wireless technology will not be solely relied upon for making operational or safety decisions. Licensees must also analyze the impact of using wireless technology with safety systems to assure transmissions do not disrupt sensitive systems. An impact analysis is necessary for implementation of wireless technology for CDAs associated with safety-related and important-to-safety systems.

The use of wireless communications for monitoring CDAs associated with SR & ITS functions is permitted with the following mitigations:

- Wireless CDAs are continuously monitored for unauthorized connections to an access point (e.g., through connection to the site SIEM and IDS).
- Wireless CDAs are isolated from other wireless communication systems (e.g., business or EP system). Information may only be sent to a lower security level (e.g., to a lower level SIEM) via wired connections through a boundary device.
- If using automated rogue wireless device detection, verify the coverage of the area containing the wireless monitoring CDAs (e.g., heat maps).
- Enforce the prohibition of changes to the wireless system to authorized personnel for making authorized changes.]

- Disabling wireless capabilities when not utilized.
- Establishes usage restrictions and implementation guidance for wireless technologies.
- Documents, justifies, authorizes, monitors, and controls wireless access to CDAs and ensures that the wireless access restrictions are consistent with defensive strategies and defensive model and articulated in the Cyber Security Plan.
- Conducts scans every 31 days in accessible areas to identify and disable unauthorized wireless access points capable of adversely affecting SSEP function.

1.18 Insecure And Rogue Connections

This Technical Cyber Security Control performs verification during deployment of CDAs, when changes or modifications occur to CDAs, and every 31 days for accessible areas, that CDAs are free of insecure (e.g., rogue) connections such as vendor connections and modems.

1.19 Access Control For Portable And Mobile Devices

This Technical cyber security control:

- Establishes and documents usage restrictions and implementation guidance for controlled portable and mobile devices.
- Authorizes, monitors, and controls device access to CDAs.
- Enforces and documents mobile device security and integrity are maintained at a level consistent with the CDA they support.
- Enforces and documents mobile devices are used in one security level and mobile devices are not moved between security levels.

1.20 Proprietary Protocol Visibility

This Technical cyber security control ensures alternative controls/countermeasures are implemented to mitigate risk associated with the use of proprietary protocols that create a lack of visibility (e.g., systems cannot detect attacks because the protocol is proprietary).

1.21 THIRD PARTY PRODUCTS AND CONTROLS

This Technical cyber security control ensures alternative controls/countermeasures are implemented to mitigate risks created by the lack of security functions provided by third party products in situations where third-party security solutions are not allowed due to vendor license and service agreements, and where loss of service support would occur if third party applications are installed without vendor acknowledgement or approval.

1.22 USE OF EXTERNAL SYSTEMS

This Technical cyber security control:

- Ensures that external systems cannot be accessed from higher levels, such as Levels 4 and 3,
- Prohibits external systems from accessing CDAs in Levels 3 and 4, and
- Prohibits users from using an external system to access CDAs or to process, store, or transmit organization-controlled information except in situations where the implementation of equivalent security measures on the external system is verified.

1.23 PUBLIC ACCESS PROTECTIONS

This security control ensures that information that could cause an adverse impact on SSEP functions or could assist an adversary in carrying out an attack is not released to the public.

2 AUDIT AND ACCOUNTABILITY

2.1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

This Technical cyber security control develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented audit and accountability policy that addresses the purpose, scope, roles, responsibilities, management commitment, and internal coordination, and
- Formal, documented procedures that facilitate the implementation of the audit and accountability policy and associated audit and accountability security controls.

2.2 AUDITABLE EVENTS

This Technical cyber security control:

- Determines and documents in conjunction with safety, security and emergency preparedness functions, which CDA related events require auditing,
- Defines the list of auditable events and frequency of auditing for identified auditable events,
- At a minimum, audits CDA connections, user login/logouts, configuration/software/firmware changes, audits setting changes, privileged access, privileged commands, and any modifications of the security functions of CDAs,
- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support the use of automated

mechanisms to generate audit records and employs non-automated mechanisms and procedures,
- Reviews and updates the list of defined auditable events at least every 12 months,
- Includes execution of privileged functions in the list of events to be audited by the CDAs,
- Prevents CDAs from purging audit event records on restart,
- Coordinates security audit functions within the facility to enhance mutual support and to help guide the selection of auditable events,
- Configures CDAs so that auditable events are adequate to support after-the-fact investigations of security incidents,
- Create and protect audit records for account creation, deletion and modification, and
- Adjusts the events to be audited within the CDAs based on current threat information and ongoing assessments of risk.

2.3 CONTENT OF AUDIT RECORDS

This Technical cyber security control:
- Ensures that CDAs produce audit records that contain sufficient information to establish what events occurred, when the events occurred, where the events occurred, the sources of the events, and the outcome of the events.
- Ensures that CDAs provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
- Implements architecture that provides the capability to centrally manage the content of audit records generated by individual components throughout CDAs, and to prevent CDAs from altering or destroying audit records.

2.4 AUDIT STORAGE CAPACITY

This Technical cyber security control allocates audit record storage capacity, meets NRC record retention requirements, and configures auditing to reduce the likelihood of such capacity being exceeded.

2.5 RESPONSE TO AUDIT PROCESSING FAILURES

This Technical cyber security control manages responses to audit processing failures by performing the following:

- For CDAs that are part of centralized logging, if audit processing capabilities fail for a CDA or security boundary device, alerts are sent to designated officials.
- If the design configuration of the CDA's supports, provide a warning when allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity. The storage volume limit is based on the function of how quickly storage capacity is consumed and the organization's resources and response times.
- Actions are taken to preserve the audit logs for record retention requirements and after-the-fact investigations.

- Auditing failures will be assessed and determination of the device functionality should follow the CAP process.
- Justification and details for alternate compensating security controls are documented for those instances in which a CDA cannot respond to audit processing failures.

2.6 AUDIT REVIEW, ANALYSIS, AND REPORTING

This Technical cyber security control:

- Reviews and analyzes the CDAs audit records every 31 days, for indications of inappropriate or unusual activity, and reports the findings to the designated official.
- Adjusts the level of audit review, analysis, and reporting within the CDAs when there is a change in risk to the safety, security and emergency preparedness functions based on credible sources of information.
- Employs automated mechanisms on CDAs to integrate audit review, analysis, and reporting processes for investigation and response to suspicious activities.

2.7 AUDIT REDUCTION AND REPORT GENERATION

This Technical cyber security control ensures CDAs are configured and deployed to do the following:

- Provide CDA audit reduction and report generation capability.
- Provide the capability to process audit records for events of interest based upon selectable, event criteria in an automated fashion.

This Technical cyber security control also documents the justification and details for alternate compensating security controls where a CDA cannot support auditing reduction and report generation by providing this capability through a separate system.

2.8 TIME STAMPS

This Technical cyber security control ensures CDAs use a time source protected at an equal or greater level than the CDAs or internal system clocks to generate time stamps for audit records, and the time on CDAs are synchronized.

The time of CDAs are synchronized from a dedicated source protected at an equal or greater level than the CDA existing on the security network, attached directly to the CDA, via a GPS-based time server or via SNTP and a trusted key management process.

Only methods of time synchronization that do not introduce a vulnerability to cyber attack and/or common-mode failure are utilized, or alternative controls are implemented to manage potential cyber security risks when time synchronization cannot be used for a CDA.

2.9 PROTECTION OF AUDIT INFORMATION

This Technical cyber security control:

- Protects audit information and audit tools from unauthorized access, modification, and deletion in a manner consistent with the CDA sources.

- Ensures that audit information is protected at the same level as the device sources.

2.10 NON-REPUDIATION

This Technical cyber security control ensures the protection of CDAs and audit records against an individual falsely denying they performed a particular action.

2.11 AUDIT RECORD RETENTION

This Technical cyber security control ensures audit record retention is consistent with record keeping requirements for the access authorization program to provide support for after-the-fact investigations of security incidents and to meet regulatory and record retention requirements.

2.12 AUDIT GENERATION

This Technical cyber security control:

For security architecture:

- Provides audit record generation capability for the auditable events on CDAs.
- Provides audit record generation capability and allows authorized users to select which auditable events are to be audited by specific components of CDAs.
- Generates audit records for the selected list of auditable events on CDAs.
- Provides the capability to compile audit records from multiple components within CDAs into a site-wide (logical or physical) audit trail that is time-correlated to within defined levels of tolerance for relationship between time stamps of individual records in the audit trail.

3 CDA, SYSTEM AND COMMUNICATIONS PROTECTION

3.1 CDA, SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

This Technical cyber security control ensures development, dissemination, and periodic reviews in accordance with 10 CFR 73.55(m), and updates of:

- Formal, documented CDA, system and communications protection policy that addresses the purpose, scope, roles, responsibilities, management commitment, and internal coordination.
- Formal, documented procedures that facilitate the implementation of the CDA, system and communications protection policy and associated CDA, system and communications protection of cyber security controls.

3.2 APPLICATION PARTITIONING/SECURITY FUNCTION ISOLATION

This Technical cyber security control:

- Configures CDAs to separate applications into user functionality (including user interface services) and CDAs management functionality.
- Configures CDAs to isolate security functions from non-security functions. This is accomplished through partitions, domains, etc., including control of access to and

integrity of the hardware, software, and firmware that perform these security functions.

- Where a CDA cannot support security function isolation implements alternative physical controls, such as:
  - Physically restricts access to the CDA,
  - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
  - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - Ensures that individuals who have access to the CDA are qualified, and
  - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

3.3 SHARED RESOURCES

This Technical cyber security control:

- Configures CDAs to prevent unauthorized and unintended information transfer via shared system resources.
- Uses physically separate network devices to create and maintain logical separation of cyber security defensive levels from each other and from all other levels.

3.4 DENIAL OF SERVICE PROTECTION

This Technical cyber security control:

- Configures CDAs to protect against or limit the effects of denial of service attacks.
- Configures CDAs to restrict the ability of users to launch denial of service attacks against other CDAs or networks.
- Configures CDAs to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding and saturation types of denial-of-service attacks.

3.5 RESOURCE PRIORITY

DELETED

3.6 TRANSMISSION INTEGRITY

This Technical cyber security control:

- Configures CDAs to protect the integrity of transmitted information.
- Employs cryptographic mechanisms to recognize changes to information during transmission and upon receipt unless otherwise protected by alternative physical measures.
- Implements mechanisms to prevent “man-in-the-middle” attacks (MITM) via the following methods:
  - Media Access Control (MAC) Address Locking - lock devices and ports via address locking to prevent MITM attacks and rogue devices from being added to the network.

  - Network Access Control (NAC) - implement NAC to prevent MITM attacks and rogue devices from being added to the network.
- Implements monitoring to detect MITM and address resolution protocol (ARP) poisoning.
- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support transmission integrity and implements the following:
  - Physically restricts access to the CDA,
  - Monitors and records physical access to the CDA to detect and respond to intrusions,
  - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - Ensures that individuals who have access to the CDA are qualified, and
  - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

3.7 TRANSMISSION CONFIDENTIALITY

This Technical cyber security control:

- Configures the CDAs to protect the confidentiality of transmitted information.
- Employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission and receipt unless otherwise protected by alternative physical measures.
- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot internally support transmission confidentiality capabilities, including Virtual Private Networks, or implements the following:
  - Physically restricts access to the CDA,
  - Monitor and record physical access to the CDA to detect and respond to intrusions,
  - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - Ensures that individuals who have access to the CDA are qualified, and
  - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

3.8 TRUSTED PATH

This Technical cyber security control configures CDAs to use trusted communication paths between the user and the security functions of CDAs, which includes authentication and re-authentication, at a minimum.

3.9 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

This Technical cyber security control:

- Manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures when cryptography is required and employed within

the CDAs in accordance with NRC Regulatory Issue Summary (RIS) 2002-15, Revision 1, "NRC Approval of Commercial Data Encryption Products for the Electronic Transmission of Safeguards Information."

- Configures CDAs to implement cryptographic mechanisms that comply with NRC Regulatory Issue Summary (RIS) 2002-15, Revision 1, NRC Approval of Commercial Data Encryption Products for the Electronic Transmission of Safeguards Information.

3.10 UNAUTHORIZED REMOTE ACTIVATION OF SERVICES

This Technical cyber security control:

- Configures CDAs to prohibit remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local user.
- Configures CDAs to provide physical disconnection of cameras and microphones in a manner that supports ease of use except where these technologies are used to control and monitor the CDA for security purposes.

3.11 TRANSMISSION OF SECURITY PARAMETERS

This Technical cyber security control configures CDAs to associate security parameters with information exchanged between CDAs.

3.12 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

This Technical cyber security control ensures public key certificates are issued under a certificate policy or obtains public key certificates under a certificate policy from an approved provider.

3.13 MOBILE CODE

This Technical cyber security control:

- Establishes usage restrictions and implementation guidance for mobile code technologies based on their potential to cause damage to CDAs if used maliciously.
- Authorizes, monitors, and controls the use of mobile code within CDAs.

3.14 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE / TRUSTED SOURCE)

This Technical cyber security control:

- Configures systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.
- Configures systems that provide name/address resolution to CDAs, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enabled verification of a chain of trust among parent and child domains.

3.15 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

This Technical cyber security control:

- Configures the systems that serve name/address resolution service for CDAs to perform data origin authentication and data integrity verification on the resolution response they receive from authoritative sources.
- Configures CDAs such that upon receipt of data to perform data origin authentication and data integrity verification on resolution responses whether or not CDAs request this service.

3.16 Architecture And Provisioning For Name / Address Resolution Service

This Technical cyber security control configures the systems that collectively provide name/address resolution service for a logical organization to be fault tolerant and segregate services (i.e., implement role separation).

3.17 Session Authenticity

This Technical cyber security control configures CDAs to provide mechanisms to protect the authenticity of communications sessions.

3.18 Thin Nodes

DELETED

3.19 Confidentiality Of Information At Rest

This Technical cyber security control configures CDAs to protect the confidentiality of information at rest.

3.20 Heterogeneity

DELETED

3.21 Fail In Known (Safe) State

DELETED

4 IDENTIFICATION AND AUTHENTICATION

4.1 Identification And Authentication Policies And Procedures

This Technical cyber security control develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, and internal coordination to positively identify potential network users, hosts, applications, services, and resources using a combination of identification factors or credentials, and

- Formal, documented procedures that facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

The identification and authentication policy and procedures provide guidance on managing both user identifiers and CDA authenticators. These items include:

- Uniquely identifying users, and processes acting on behalf of a user,
- Verifying the identity of users, and processes acting on behalf of a user,
- Receiving authorization to issue a user identifier from an appropriate authorized representative,
- Ensuring that the user identifier is issued to the intended party,
- Disabling user identifier within 31 days of inactivity,
- Archiving user identifiers,
- Defining initial authenticator content,
- Establishing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators,
- Changing default authenticators upon control system installation, and
- Changing/refreshing authenticators periodically.

4.2 USER IDENTIFICATION AND AUTHENTICATION

This Technical cyber security control:

- Implements identification and authentication technology to uniquely identify and authenticate individuals and processes acting on behalf of users interacting with CDAs. Ensure that CDAs, security boundary devices, physical controls of the operating environment, and individuals interacting with CDAs, are uniquely identified and authenticated and that processes acting on behalf of users are equally authenticated and identified.
- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support user identification and authentication and implements the following:
  - Physically restricts access to the CDA,
  - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
  - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - Ensures that individuals who have access to the CDA are qualified, and
  - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.
- When exercised, multifactor authentication utilizes protected processing levels.
- Implements secure domain-based authentication and:
  - Maintains domain controllers within the given security level they are meant to service.
  - Physically and logically secures domain controllers to prevent unauthorized access and manipulation.

  - Prohibits domain trust relationships between domains that exist at different security levels.
  - Prohibits domain authentication protocols from being passed between boundaries.
  - Implements role-based access control where possible to restrict user privileges to those required to perform the task.
- Where domain-based authentication is not used:
  - Document and justify reasoning for not implementing secure domain-based authentication.
  - Implement localized authentication when feasible.
  - Implement the strongest possible challenge-response authentication mechanism within a scenario as supported by the application.
  - Implement role-based access control where possible to restrict user privileges to those required to perform the task.

4.3 PASSWORD REQUIREMENTS

This Technical cyber security control ensures that when used, passwords meet the following requirements:

- Length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the CDA.
- Passwords have length and complexity for the required security.
- Passwords are changed every 92 days.
- Passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters.
- Copies of master passwords are stored in a secure location with limited access.
- Authority to change master passwords is limited to authorized personnel.

4.4 NON-AUTHENTICATED HUMAN MACHINE INTERACTION (HMI) SECURITY

This Technical cyber security control:

- Ensures that where an HMI for a CDA cannot support authentication due to operational requirements, physical security controls exist that ensure operators are both authorized and identified, and are monitored to ensure that operator actions are audited and recorded.
- Controls access to non-authenticated human machine interactions (NHMI) so as to not hamper human-machine interaction while maintaining security of the NHMI, and ensuring that access to the NHMI is limited to authorized personnel.
- Verifies that safety, security and emergency preparedness functions are not adversely affected by authentication, session lock or session termination controls.
- Implements auditing capability on NHMIs to ensure that operator activity is recorded and monitored by authorized and qualified personnel. These historical records are maintained to provide for auditing requirements.

4.5 DEVICE IDENTIFICATION AND AUTHENTICATION

This Technical cyber security control:

- Implements and documents technology that identifies and authenticates devices (i.e., tester) before those devices establish connections to CDAs.
- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support device identification and authentication (e.g., serial devices) and implements the following:
  - Physically restricts access to the CDA,
  - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
  - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - Ensures that individuals who have access to the CDA are qualified, and
  - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

4.6 IDENTIFIER MANAGEMENT

This Technical cyber security control manages and documents user identifiers by performing the following:

- Uniquely identifying users;
- Verifying the identity of users;
- Receiving authorization to issue a user identifier from an organization official;
- Issuing the user identifier to the intended party;
- Disabling the user identifier within 31 days of inactivity; and
- Archiving user identifiers consistent with records retention for the access authorization program.

4.7 AUTHENTICATOR MANAGEMENT

This Technical cyber security control manages CDA authenticators by performing the following:

- Defining initial authenticator content, such as defining password length and composition, tokens, keys and other means of authenticating;
- Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
- Changing default authenticators upon CDA installation; and
- Changing/refreshing authenticators every 12 months.

4.8 AUTHENTICATOR FEEDBACK

This Technical cyber security control:

- Ensures that CDAs obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
- Ensures that CDAs and feedback from CDAs do not provide information that would allow an unauthorized user to compromise the authentication mechanism.

4.9 CRYPTOGRAPHIC MODULE AUTHENTICATION

This Technical cyber security control ensures that CDAs authenticate cryptographic modules in accordance with NRC Regulatory Issue Summary (RIS) 2002-15, Revision 1, "NRC Approval of Commercial Data Encryption Products for the Electronic Transmission of Safeguards Information."

5 SYSTEM HARDENING

5.1 REMOVAL OF UNNECESSARY SERVICES AND PROGRAMS

This Technical cyber security control documents required applications, utilities, system services, scripts, configuration files, databases, and other software and the appropriate configurations, including revisions and/or patch levels for the computer systems associated with the CDAs.

This Technical cyber security control maintains a list of services required for CDAs. The listing includes necessary ports and services required for normal and emergency operations. The listing also includes an explanation or cross reference to justify why a service is necessary for operation and those services and programs that are necessary for operation are allowed.

This Technical cyber security control verifies and documents that CDAs are patched or mitigated in accordance with the patch management process and security prioritization timelines according to NEI 08-09, Revision 7, Appendix E, Section 3.2, Flaw Remediation.

This Technical cyber security control documents the remediation period appropriate for software and service updates and/or workarounds to mitigate vulnerabilities associated with the product, and to maintain the established level of security.

This Technical cyber security control documents the operating system and software patches as CDAs evolve to allow traceability and to verify no extra services are reinstalled or reactivated.

This Technical cyber security control removes and/or disables software components that are not required for the operation and maintenance of the CDA prior to incorporating the CDA into the production environment. This technical cyber security control documents what components were removed and/or disabled. The software removed and/or disabled includes, but is not limited to:

- Device drivers for network devices not delivered
- Device drivers for unused peripherals
- Unused removable media support
- Messaging services (e.g. MSN, AOL IM, etc.)
- Servers or clients for unused services
- Software compilers in user workstations and servers except for development workstations and servers
- Software compilers for languages that are not used in the control system
- Unused networking and communications protocols

- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used during system development
- Unused data and configuration files
- Sample programs and scripts
- Unused document processing utilities (Microsoft Word, Excel, Power Point, Adobe Acrobat, OpenOffice, etc.)
- Games

5.2 HOST INTRUSION DETECTION SYSTEM (HIDS)

This Technical cyber security control establishes, implements, and documents requirements to:

- Configure HIDS to include attributes such as: static file names, dynamic file name patterns, system and user accounts, execution of unauthorized code, host utilization, and process permissions to enable the system to detect cyber attacks up to and including the DBT.
- Configure HIDS so system and user account connections are logged. This log is configured such that the operator or security personnel are alerted if an abnormal situation occurs.
- Configure HIDS in a manner that does not adversely impact the CDA/CS safety, security and emergency preparedness functions.
- Configure security logging storage devices as "append only" to prevent alteration of records on those storage devices.
- Perform rules updates and patches to the HIDS as security issues are identified to maintain the established level of system security.

This Technical cyber security control secures HIDS configuration documents to ensure that they are inaccessible to unauthorized personnel.

5.3 CHANGES TO FILE SYSTEM AND OPERATING SYSTEM PERMISSIONS

This Technical cyber security control establishes, implements, and documents requirements to:

- Configure CDAs with least privilege, data, commands, file and account access.
- Configure the system services to execute at the least privilege level possible for that service and documents the configuration.
- Document the changing or disabling of access to files and functions.
- Validate baseline permission and security settings are not altered after modifications or upgrades.

5.4 HARDWARE CONFIGURATION

This Technical cyber security control establishes, implements, and documents requirements to:

- Disable through software or physical disconnection, unneeded communication ports and removable media drives, or provided engineered barriers.
- Password protects the BIOS from unauthorized changes.

- Document mitigation measures in cases that password protection of the BIOS is not technically feasible.
- Document the hardware configuration (disabled or removed USB ports, CD/DVD drives, and other removable media devices).
- Use network devices to limit access to/from specific locations, where appropriate.
- Allow system administrators the ability to re-enable devices if the devices are disabled by software and document the configuration.
- Verify that replacement devices are configured equal to or better than the original.

5.5 INSTALLING OPERATING SYSTEMS, APPLICATIONS, AND THIRD-PARTY SOFTWARE UPDATES

This Technical cyber security control establishes, implements, and:

- Documents the patch management program, update process, and individuals responsible for installation;
- Documents notification of vulnerabilities affecting CDAs to be conducted within the maximum periodicity defined in the risk determination;
- Documents notification to authorized personnel of patches affecting cyber security;
- Documents the authorization of updates or workarounds to the baseline before implementation;
- Documents the patch management process for the CDA after installation. The policies, procedures, and programs include mitigation strategies for instances when the vendor of the CDA recommends not to apply released patches;
- Documents the level of support for testing patch releases;
- Tests received cyber security updates on a non-production system for testing and validation prior to installing on production systems when practical, and
- Tests updates for security impact.

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX E: OPERATIONAL AND MANAGEMENT CYBER SECURITY CONTROLS

The Operational and Management Cyber Security Controls in this appendix represent methods for the mitigation of risks to digital systems. When implementing cyber security controls, discretion may be taken with the means by which the control is implemented. When a control or aspects of a control are not implemented, an analysis is performed to ensure that the risk is effectively mitigated. A security control is considered to be applied when there is high assurance that the CDA is adequately protected from the risk considered by the security control. Section 3.1.6 of NEI 08-09, Revision 7, Appendix A, provides a multi-step process for the analysis and documentation of the application of cyber security controls.

Security Controls are elements of the Security Program and are reviewed consistent with the requirements of 10 CFR 73.55(m).

1 MEDIA PROTECTION

1.1 MEDIA PROTECTION POLICY AND PROCEDURES (SGI, NON-SGI AND 2.390)

This security control develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance for information categories as defined by the site policies. If the media can provide information to assist an adversary, it must be marked at a minimum to identify and to identify the sensitive nature of the media.
- A formal, documented procedure to facilitate the implementation of the media protection policy and associated media protection controls which include the methodology that defines the purpose, scope, roles, responsibilities, and management commitment in the areas of media receipt, storage, handling, sanitization, removal, reuse, and disposal necessary to provide a high assurance that the risk of unauthorized disclosure of information that could be used in a cyber attack to adversely impact the safety, security, and emergency preparedness functions of the nuclear facility is prevented.

1.2 MEDIA ACCESS

Access to CDA media is documented and restricted to authorized individuals. CDA media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm).

Access to any security information on mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) is restricted to authorized individuals.

Automated mechanisms, when possible, are employed to restrict access to media storage areas. Access attempts and accesses granted are audited.

1.3 MEDIA LABELING/MARKING

Removable CDA media and CDA output are marked according to information categories indicating the distribution limitations and handling caveats. Output on external media, including video display devices, is marked in accordance with the identified set of special dissemination, handling, or distribution instructions that apply to system output using human readable, standard naming conventions for media labels.

1.4 MEDIA STORAGE

CDA media are physically protected and securely stored to a level commensurate with the determination of the sensitivity of the data.

1.5 MEDIA TRANSPORT

CDA media in transport is physically protected, transported and stored to a level commensurate with the security classification of the data:

- CDA media is protected and controlled during transport and restricts the activities associated with transport of such media to authorized personnel.
- Digital and non-digital media is protected during transport outside of controlled areas using defined security measures (e.g., locked containers, security details, cryptography).
- Activities associated with the transport of CDA media are documented using a defined system of records.
- An identified custodian is utilized during transport of CDA media.

1.6 MEDIA SANITATION AND DISPOSAL

CDA media, both digital and non-digital, are sanitized prior to disposal or release for reuse:

- CDA media requiring sanitization are identified, and the appropriate techniques and procedures (e.g., NIST SP 800-88) to be used in the process. Identified CDA media, both paper and digital, are sanitized prior to disposal or release for reuse.
- Media sanitization and disposal actions are tracked, documented, and verified, and every 92 days tests are performed on sanitized data to ensure equipment and procedures are functioning properly.

2 PERSONNEL SECURITY

2.1 PERSONNEL SECURITY POLICY AND PROCEDURES

A reviewing official grants unescorted access or certifies unescorted access authorization to those individuals who have access, extensive knowledge, or administrative control of CDAs or communication systems that can adversely impact safety, security, emergency preparedness functions, prior to them gaining access to those systems, in accordance with 10 CFR 73.56.

2.2 PERSONNEL TERMINATION/TRANSFER

Upon termination/transfer of an individual's employment, the access authorization program established per 10 CFR 73.56 is followed and the following are performed:

- Terminate CDA and system access;
- As applicable, conduct exit interviews;
- Retrieve cyber security-related organizational property; and
- Retain access to organizational information and CDAs formerly controlled by terminated/transferred individual.

3 SYSTEM AND INFORMATION INTEGRITY

3.1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

This security control develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updates a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance. A formal, documented procedure is in place to facilitate the implementation of CDAs and information integrity policy and associated system and information integrity controls.

System and information integrity procedures consider and address the following attributes:

- Detect malicious or suspicious access control and/or networking anomalies occurring at established defensive level boundaries and within security levels,
- Alert appropriate staff to the detected malicious or suspicious activity using a secure communications mechanism that is protected from the network being monitored,
- Isolate and contain malicious activity,
- Neutralize malicious activity,
- Centralize logging of cyber security events to support correlations,
- Provide for secure monitoring and management of security mechanisms,
- Provide time synchronization for security-related devices, and
- Provide high assurance that the physical and logical security of the monitoring network (or systems) matches or exceeds and differs from the systems or networks being monitored.

3.2 FLAW REMEDIATION

This security control establishes, implements, and documents procedures to:

- Identify the security alerts and vulnerability assessment process,
- Communicate vulnerability information,
- Correct security flaws in CDAs, and
- Perform vulnerability scans or assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production.

Before implementing corrections, software updates related to flaw remediation are documented and tested to determine the effectiveness and potential side effects on CDAs. Flaw remediation information is captured in the Corrective Action Program.

3.3 MALICIOUS CODE PROTECTION

Real-time malicious code protection mechanisms are established, deployed, and documents at security boundary device entry and exit points, CDAs (if applicable), workstations, servers, and mobile computing devices (i.e., calibrators) on the network to detect and eradicate malicious code resulting from:

- Data communication between systems, CDAs, removable media, or other common means; and
- Exploitation of CDAs vulnerabilities.

Malicious code protection mechanisms (including signature definitions) are documented and updated whenever new releases are available in accordance with programs, procedures, and processes.

Malicious code protection mechanisms are documented and configured to:

- Perform periodic scans of security boundary devices, CDAs (if applicable), workstations, servers, and mobile computing devices at an interval commensurate with risk determination, and real-time scans of files from external sources as the files are downloaded, opened, or executed, and
- Disinfect and quarantine infected files.

Malicious code protection software products from multiple vendors are documented and employed as part of defense-in-depth, and the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system are addressed.

Malicious code protection mechanisms are centrally managed.

The CDAs prevents users from circumventing malicious code protection capabilities.

The CDAs update malicious code protection mechanisms when directed by a privileged user.

Users are not allowed to introduce unauthorized removable media into the CDAs.

Media interfaces (e.g., USB ports) that are not required for the operation of the CDA are disabled.

Malicious code protection mechanisms are documented and implemented to identify data containing malicious code and responded accordingly when CDAs encounters data not allowed by the security policy.

3.4 MONITORING TOOLS AND TECHNIQUES

This security control consists of:

- Monitoring events on CDAs
- Detecting attacks on CDAs
- Detecting and blocking unauthorized connections
- Identifying unauthorized use of CDAs
- Monitoring devices that are deployed to provide visibility across CDAs for the following capabilities:
    - To collect information to detect attacks, unauthorized behavior and access, authorized access, and
    - To track specific types of transactions of interest
- The level of monitoring activity is heightened whenever there is an indication of increased risk to safety, security, or emergency operations of the site when determined by site security personnel or by the NRC.
- Individual intrusion detection tools are documented, interconnected, and configured into a plant-wide intrusion detection system using common protocols.
- Automated tools are documented and employed to support near-real-time analysis of events.
- Automated tools are documented and employed to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
- Inbound and outbound communications are monitored, and logged, for unusual or unauthorized activities or conditions and the monitoring capabilities provide real-time alerts when indications of compromise or potential compromise occur.
- Users are prevented from circumventing intrusion detection and prevention capabilities.
- Incident response personnel notify and document suspicious events and the least-disruptive actions (as determined by policy and risk determination) to safety, security and emergency preparedness functions are taken to investigate and terminate suspicious events.
- Information obtained from intrusion monitoring tools is documented and protected from unauthorized access, modification, and deletion.
- Competent cyber security personnel randomly test and document cyber security intrusion monitoring tools.
- Cyber intrusion detection and prevention systems are functionally tested (e.g., test that verifies that signatures are functioning, such as the use of a benign virus signature file) every 7 days, and before being placed back in service after each repair or inoperative state.
- Provisions are documented and made to ensure that encrypted traffic is visible to monitoring tools.
- Outbound communications traffic is analyzed at the external boundary of CDAs (i.e., system perimeter) and, as necessary, at selected interior points within CDAs to discover anomalies.

- The use of monitoring tools and techniques are employed to verify that the functional performance of CDAs is not adversely impacted and that, where monitoring tools and techniques cannot be used, alternate controls are in place to compensate.

3.5 SECURITY ALERTS AND ADVISORIES

This security control consists of:

- Receiving security alerts, bulletins, advisories, and directives from credible licensee-designated external organizations on an ongoing basis, such as third party security alert notification services and vendor security alert lists;
- Independently evaluating and determining the need, severity, methods and time frames for implementing security directives consistent with the cyber security controls for the CDA.
- Within time frames established above:
  - Generating and documenting internal security alerts, advisories, and directives as necessary;
  - Disseminating and documenting security alerts, advisories, and directives to designated personnel for action and tracking their status and completion;
  - Implementing and documenting security directives in accordance with time frames established above, or implementing an alternate security measure;
  - Implementing and documenting any required mitigation measures in accordance with the configuration management process;
  - Employing automated or other mechanisms (e.g., e-mail lists) to make security alert and advisory information available to the appropriate site personal, as needed.

3.6 SECURITY FUNCTIONALITY VERIFICATION

The correct operation of security functions of CDAs are verified and documented, periodically in accordance with 10 CFR 73.55(m), upon startup and restart, upon command by a user with appropriate privilege, and when anomalies are discovered, where possible.

When technically feasible, CDAs provide notification of failed security tests and these failed tests are documented.

If technically feasible, CDAs provide automated support for the management of distributed security testing and the results of this testing are documented.

The justification for employing alternative (compensating) controls is documented where a CDA cannot support the use of automated mechanisms for the management of distributed security testing. Non-automated mechanisms and procedures to test security functions include the use of:

- Qualified individuals;
- Trustworthy and reliable individuals in accordance with 10 CFR 73.56;
- Test procedures and results;
- Physically restricted access to the CDA;

- Monitored and recorded physical access to the CDA (for detection and response to intrusions), and
- Auditing/validation measures (e.g., security officer rounds, periodic monitoring of tamper seals).

3.7 SOFTWARE AND INFORMATION INTEGRITY

This security control consists of:

- Detecting and documenting unauthorized changes to software and information;
- Employing hardware access controls (e.g., hardwired switches), where technically feasible, to prevent unauthorized software changes;
- Reassessing and documenting the integrity, operation and functions of software and information by performing regular integrity, operation and functional scans, every 92 days;
- Employing and documenting automated tools, where technically feasible, that provide notification to designated individuals upon discovering discrepancies during integrity verification;
- Employing and documenting centrally managed integrity verification tools;
- Requiring the use of physical tamper evident packaging or seals for system components;
- Requiring, when tamper evident packaging is used, that seals be inspected on a regular basis, and
- Ensuring and documenting that the use of integrity verification applications does not adversely impact the operational performance of the CDA, and applying alternate controls where integrity verification applications cannot be used.

3.8 INFORMATION INPUT RESTRICTIONS

This security control consists of:

- Restricting the capability to input information to CDAs to authorized sources;
- Checking information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. Rules for checking the valid syntax of CDA inputs (e.g., character set, length, numerical range, acceptable values) are documented and in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are pre-screened to prevent the content from being interpreted as commands.

3.9 ERROR HANDLING

Controls for CDAs are documented and implemented so that:

- Error conditions are identified;
- Generated error messages provide information necessary for corrective actions without revealing harmful information that could be exploited by adversaries;
- Error messages are revealed to authorized personnel;
- Inclusion of sensitive information, such as passwords, in error logs or associated administrative messages is prohibited.

3.10 INFORMATION OUTPUT HANDLING AND RETENTION

Sensitive information obtained from a CDA is not disclosed to unauthorized personnel and is handled and disposed of such that output is not disclosed to unauthorized personnel.

3.11 ANTICIPATED FAILURE RESPONSE

The availability of a CDA is protected through compliance with current licensing basis (e.g., Technical Specifications, Preventive Maintenance Program, Maintenance Rule Program, Security Plans, Emergency Plan, Corrective Action Program). Where these programs do not apply, the availability of a CDA is provided by:

- Substitute components, when needed, and a mechanism to exchange active and standby roles of the components, and by
- Considering the mean time to failure for components in specific environments of operation.

4 MAINTENANCE

4.1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

This security control develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, CDA maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, associated system maintenance controls, and compliance.
- Formal, documented procedures to facilitate the implementation of the CDA maintenance policy and associated system maintenance controls.
- The system maintenance policy and procedures include CDAs located in security boundaries:
  - Owner Controlled Areas: The outermost security area boundary for a plant that is outside the plant's security area.
  - Protected Areas: An area within the boundaries of a nuclear power plant that is encompassed by physical barriers and to which access is controlled (see 10 CFR 73.2).
  - Public Access Areas: Locations outside the physical control of the plant.

4.2 MAINTENANCE TOOLS

This security control consists of:

- Approving, monitoring and documenting the use of digital maintenance tools used to maintain CDAs.
- Controlling maintenance tools associated with CDAs to prevent improper modifications. Maintenance tools include, for example, diagnostic and test equipment and mobile devices such as laptops.
- Checking and documenting media and mobile devices, such as laptops, containing diagnostic, system and test programs/software for malicious code before the media or mobile device is used in/on CDAs.

- Controls the removal of maintenance equipment by one of the following:
  - Retaining the equipment within the licensee control,
  - Obtaining approval from an authority authorizing removal of the equipment from the licensee control, or
  - Verifying that there is no licensee proprietary information contained on the equipment and validating the integrity of the device before reintroduction into the licensee control. If unable to verify/validate the integrity of the device, then sanitize or destroy the equipment.
- Employing automated or manual mechanisms to restrict the use of maintenance tools to authorized personnel; employs manual mechanisms where CDAs or support equipment (e.g., laptops) cannot support automated mechanisms.

4.3 PERSONNEL PERFORMING MAINTENANCE AND TESTING ACTIVITIES

This security control consists of:

- Maintaining and documenting a current list of authorized maintenance personnel consistent with its access authorization program and insider mitigation program, and
- Implementing and documenting automated mechanism or non-automated mechanism to detect unauthorized use or execution of commands by an escorted individual, or
- Designating and documenting personnel with required access authorization and knowledge necessary to supervise escorted personnel interacting with CDAs.

5 PHYSICAL ENVIRONMENT PROTECTION

This family of security controls implements and documents physical protections for CDAs located outside the protected area. Physical protections for CDAs located inside the protected area are provided by the Physical Security Plan to comply with 10 CFR 73.55.

5.1 PHYSICAL PROTECTION POLICIES AND PROCEDURES

This security control develops, implements, reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented physical protection policy that addresses:
  - The purpose of the physical security program as it relates to protecting the CDAs;
  - The scope of the physical security program as it applies to the organization's staff and third-party contractors;
  - The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with security policies and other regulatory commitments.
- Formal, documented procedures to facilitate the implementation of the physical protection policy and associated physical protection security controls.

5.2 THIRD PARTY/ESCORTED ACCESS

This security control consists of:

- Screening, enforcing and documenting security controls for third-party personnel and monitoring service provider behavior and compliance. Third-party providers include

service contractors and other organizations providing control system operation and maintenance, development, IT services, outsourced applications, and network and security management.
- Including personnel security controls in acquisition-related contract and agreement documents.

5.3 PHYSICAL PROTECTION

This security control consists of securing and documenting physical access to CDAs. Physical security controls (e.g., physically isolate environment, locked doors, etc.) are employed to limit access to CDAs.

5.4 PHYSICAL ACCESS AUTHORIZATIONS

This security control consists of:
- Developing and maintaining a list of, and issuing authorization credentials (e.g., badges, identification cards, smart cards) to, personnel with authorized access to facilities containing CDAs and security boundary systems.
- Designating officials within the organization to review and approve the above access lists and authorization credentials, consistent with the access authorization program.

5.5 PHYSICAL ACCESS CONTROL

This security control consists of:
- Controlling physical access points (including designated entry/exit points) to locations where CDAs reside and verifies individual access authorization before granting access these areas.
- Approving individual access privileges and enforces physical and logical access restrictions associated with changes to CDAs.
- Controlling logical access through the use of electronic devices and software.
- Generating, retaining, and reviewing records pertaining to access restrictions.
- Ensuring qualified and authorized individuals obtain access to CDAs.
- Controlling physical access to the CDAs independent of the physical access controls for the facility.

5.6 ACCESS CONTROL FOR TRANSMISSION MEDIUM

This security control consists of controlling and documenting physical access to CDA communication paths.

5.7 ACCESS CONTROL FOR DISPLAY MEDIUM

This security control consists of controlling and documenting physical access to CDAs that display information that may assist an adversary to prevent unauthorized individuals from observing the display output.

5.8 MONITORING PHYSICAL ACCESS

This security control consists of:

- Monitoring and documenting physical access to CDAs and security boundaries to detect and respond to physical security incidents. For incidents, reviews physical access logs and coordinates results of reviews and investigations with the incident response personnel.
- Monitoring real-time physical intrusion alarms and surveillance equipment.
- Employing automated mechanisms to assess and recognize potential intrusions and initiates appropriate response actions.
- Providing lighting for access monitoring devices (e.g., cameras).

5.9 VISITOR CONTROL ACCESS RECORDS

This security control consists of:

- Controlling and documenting visitor physical access to CDAs by verifying the identity and confirming access authorization of these individuals prior to entry.
- Escorting visitors and monitoring visitor activity to prevent adverse impact to safety, security and emergency preparedness functions.

6 DEFENSE-IN-DEPTH

This security control implements and documents a defensive strategy that:

- Allocates the appropriate degree (i.e., level 4, 3, etc.) of cyber security protection to CDAs that carry out safety, important-to-safety, security, and emergency preparedness functions, and protect those CDAs from lower defensive levels.
- Controls/restricts remote access to CDAs located in the highest defensive level.
- Allocates at least the second highest degree of cyber security protection (i.e., level 3) to CDAs providing data acquisition functions and protect those CDAs from lower defensive levels.
- Allows only one-way direct data flow from the more secure to less secure security levels in accordance with Section 4.3 of the licensee's CSP.
- Ensures that data flow from one level to other levels occurs through a device that enforces the security policy between levels and detect, prevent, delay, mitigate, and recover from a cyber attack coming from the lower security level.
- Ensures that direct communications between digital assets at lower security levels and digital assets at higher security levels are eliminated or restricted with justification that explains that communication from a lower security level to a higher security level verifies that a compromise of such communication will not prevent or degrade the functions performed by the CDAs in the higher security level.
- Moves data, software, firmware and devices from lower levels of security to higher levels of security using a documented validation process or procedure. The validation process or procedure is trustworthy at or above the trusted level of the device the data, code, information or device is installed on or connected with to ensure that the data, software, firmware or devices are free from known malicious code, Trojans viruses, worms and other passive attacks.

In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:

- Physically and logically secure and harden CDAs to prevent unauthorized access or manipulation.
- Employ secure management communications and encryption per Appendix D of this NEI 08-09, Revision 7.
- Provide logging and alert capabilities.
- Detect and prevent malware from moving between boundaries.
- Are capable of performing more than stateful inspection with respect to the protocols used in communication across the boundary, such as through a bastion host or application proxy.
- Except in the case of data diodes, contain a rule set that at a minimum:
  - Is configured to deny traffic, except that which are authorized;
  - Provides protocol, source, and destination filtering such as IP addresses, MAC addresses, TCP ports, and UDP ports;
  - Bases blocking on source and destination address pairs, services, and ports where the protocol supports this;
  - Does not permit either incoming or outgoing traffic by default;
  - Are managed either through a direct connection to the firewall from a management device, such as a laptop computer, or through a dedicated interface connected to a site-centric security network;
  - Does not permit direct communication to the firewall from any of the managed interfaces;
  - Records information relative to accepted and rejected connections, traffic monitoring, analysis, and intrusion detection;
  - Forwards logs to a centralized logging server;
  - Enforces destination authorization. Users are restricted and allowed to reach the CDAs necessary for their function;
  - Records information flow for traffic monitoring, analysis, and intrusion detection;
  - Is deployed and maintained by authorized personnel trained in the technologies used;
  - Documents and designs with minimal connections that permit acquisition and control networks to be severed from corporate networks, should that decision be made, in times of cyber attacks or when directed by authorized personnel who are designated to do so;
  - Is evaluated, analyzed, and tested prior to deployment and upon modification of the rule set and/or updates to the operational software and firmware required to operate the firewall;
  - Receives time synchronization from a trusted and dedicated source;
  - Time is synchronized with CDAs to provide for event correlation;
  - Are capable of forwarding logging information in a standard format to a secure logging server or uses an external device to provide this logging (as in the case of a data diode);
  - Logs are reviewed by personnel that are trained in such analysis to detect malicious or anomalous activity;

- Are updated every 92 days;
- Uses physically and logically secured and hardened computing devices and flow control to prevent unauthorized access, or manipulation of data streams;
- Allows no information of any kind, including handshaking protocols, to be transferred directly (i.e., without traversing the boundary control device) from networks or systems existing at the less secure level to networks or systems existing at the more secure level;
- Employs measures to prevent viruses or other malicious or unwanted programs from propagating information between security levels.

7 ATTACK MITIGATION AND INCIDENT RESPONSE

7.1 INCIDENT RESPONSE POLICY AND PROCEDURES

The security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance.
- Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls that establish procedures for:
  - Notifying staff and operators,
  - Determining whether unexpected indications or fault conditions could be the result of a cyber attack in progress,
  - In the event that the cyber attack was the result of previous activities that have lain dormant within a CDA, use the Corrective Action Program to perform an analysis to identify entry mechanisms and take steps to close down the vulnerability,
  - Establishing a disaster recovery plan that permits recovery from a cyber attack. System backups are an essential part of this Plan and allow rapid reconstruction of the CDA.

Recovery plans are exercised to demonstrate they are effective and that personnel are familiar with how to employ them in accordance with plant plans (e.g., disaster recovery plans, business continuity plans, emergency plans). Changes are made to recovery plans based on lessons learned from exercises and drills and actual incidents and events.

Stakeholders are included in the development of incident response policies, procedures and plans, including the following groups:

- Physical security
- Cyber security team
- Operations
- Engineering
- Information Technology
- Human resources

- System support vendors
- Management
- Legal
- Safety

7.2 INCIDENT RESPONSE TRAINING

This security control consists of:

- Training personnel in their incident response roles and responsibilities with respect to the Incident Response procedures and providing refresher training at least annually.
- Incorporating simulated events into incident response training to facilitate effective response by personnel in crisis situations.
- Documenting incident response training exercises and acknowledgements that personnel are qualified and trained.

7.3 INCIDENT RESPONSE TESTING AND DRILLS

This security control consists of:

- Testing and conducting drills of the incident response capability for CDAs annually.
- Using site-defined tests and/or drills to update the incident response capability to maintain its effectiveness.
- Documenting the results of testing and drills.
- Providing incident response testing and drills procedures.
- Employing automated mechanisms to test/drill the incident response capability.
- Performing and documenting announced and unannounced tests and drills.

7.4 INCIDENT HANDLING

This security control consists of:

- Implementing and documenting ongoing incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery.
- Incorporating lessons learned from ongoing incident handling activities into incident response procedures, and implements the procedures accordingly.
- Forming an integrated Cyber Security Incident Response Team (CSIRT).
- Providing the team the technical skills and authority to respond to a potential cyber security event.
- Developing and documenting processes, procedures and controls that the team will employ upon the discovery or identification of a potential or actual cyber security attack.
- Documenting and defining response to the following:
  - Identification of what constitutes a cyber security incident.
  - Identification of threat level classification for incidents.
  - Description of actions to be taken for components of the Incident Response process.

- Description of individual postulated classes or categories of incidents or attacks as analyzed during the Cause Analysis performed under the Corrective Action Program (e.g. common cause, apparent cause, root cause).
- Identification of defensive strategies that would assist in identifying and containing a cyber attack.
- Description of the CSIRT incident notification process.
- Description of incident documentation requirements.
- As necessary, establishment of coordinated and secure communication methods to be used between local and remote CSIRT members and outside agencies.
- Description of response escalation requirements.

The CSIRT consists of individuals with knowledge and experience in the following areas:

- Information and digital system technology – This covers the areas of cyber security, software development and application, computer system administration, and computer networking. In particular, knowledge is required of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant business systems. In the plant operations area, this includes programmable logic controllers, control systems, and distributed control systems. In the business area, this includes computer systems and databases containing information used to design, operate, and maintain CDAs. In the networking arena, knowledge is required of both plant- and corporate-wide networks. An experienced and skilled cyber security staff member might have expertise in these areas.

- Nuclear power plant operations, engineering, and safety – This includes knowledge of overall facility operations and plant technical specifications. Staff representing this technical area must be able to trace the impact of a vulnerability or series of vulnerabilities in a CDA (or connected digital asset) outward through plant subsystems and systems so that the overall impact on safety, security, and emergency preparedness of the plant can be evaluated.

- Physical and operational security – This includes in-depth knowledge of the plant's physical and operational security program. In addition to the above requirements, specialized in-depth cyber security skills are required to perform the electronic validation testing and optional scanning activities.

- Ancillary Personnel – may not have on-site personnel trained and experienced in this arena. If this expertise is not available on site, corporate-level cyber security personnel, an independent cyber security organization, or other sources of the necessary validation expertise may be considered.

In addition, individuals with the following roles join the CSIRT on an as-needed basis depending on the incident:

- Site security (physical),
- Senior plant management,

- Corporate public relations, and
- Corporate legal.

Incident data collected includes the following:

- Incident title
- Date of incident
- Reliability of the incident report
- Type of incident (e.g., accident, virus)
- Entry point (e.g., Internet, wireless, modem)
- Perpetrator
- Type of system and hardware impacted
- Brief description of incident
- Impact on organization
- Measures to prevent recurrence
- References

7.5 INCIDENT MONITORING

Security incidents are tracked and documented on an on-going basis using automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

7.6 INCIDENT RESPONSE ASSISTANCE

This security control consists of:

- Providing year-round, 24 hours per day, competent and trained incident response support personnel who offers advice and assistance to users of CDAs in response to and reporting of cyber security incidents. The support resource is an integral part of incident response capability.
- Mechanisms are employed to increase the availability of incident response-related information and support.

8 CYBER SECURITY CONTINGENCY PLAN (CONTINUITY OF OPERATIONS)

8.1 CONTINGENCY PLAN

This security control consists of:

- Implementing a cyber security contingency plan to maintain the safety, security and emergency preparedness functions by developing and disseminating roles, responsibilities, assigned individuals with contact information, and activities associated with restoring CDAs after a disruption or failure.
- Coordinating contingency plan development with organizations responsible for related plans (e.g., Emergency Plan, Physical Security Plan) and requirements (e.g., Technical Specifications).
- Deploying CDAs such that, in the event of a loss of processing within a CDA or a loss of communication with operational facilities, CDAs will execute predetermined

actions (e.g., alert the operator and do nothing, alert the operator and then safely shut down the process, alert the operator and maintain last operational setting).

8.2 CONTINGENCY PLAN TESTING

This security control consists of:

- Testing and/or exercising and documenting the contingency plan at documented intervals to verify its effectiveness and the organization's readiness to execute this Plan.
- Reviewing the contingency plan test/exercise results and initiates appropriate corrective actions.
- Coordinating contingency plan testing and/or exercises with elements responsible for related plans.
- Testing and/or exercising and documenting the contingency plan at emergency and/or backup sites to familiarize contingency personnel with these facilities and their available resources, and to evaluate the site's capabilities to support contingency operations.
- Employing automated mechanisms to test/exercise the contingency plan by providing coverage of contingency issues, and selecting test/exercise scenarios and environments.
- Including recovery and reconstitution of CDAs as part of contingency plan testing.
- Establishing and documenting alternate controls where the contingency plan cannot be tested or exercised on production CDAs due to the potential for a significant adverse impact on safety, security, performance or reliability of the CDA.
- Using scheduled and unscheduled system maintenance activities, including responding to CDA component and system failures, as an opportunity to test or exercise the contingency plan.

8.3 CONTINGENCY TRAINING

This security control consists of:

- Training personnel in their contingency roles and responsibilities with respect to the CDAs and provides refresher training annually, or consistent with the existing contingency program, whichever period is shorter.
- Maintaining training procedures and documents training records of individuals.
- Including training drills to familiarize contingency personnel with the facility, CDAs and available resources and to evaluate the site's capabilities to support contingency operations.
- Ensuring thorough coverage of contingency issues.
- Selecting realistic test/drill scenarios and environments.

8.4 ALTERNATE STORAGE SITE/LOCATION FOR BACKUPS

Alternate storage locations are identified and documented, and the necessary agreements to permit the storage of CDA backup information are initiated. The frequency of CDA backups and

the transfer rate of backup information to the alternate storage locations are consistent with the recovery time objectives and recovery plan objectives.

This security control also consists of:

- Identifying an alternate storage location that is geographically separated from the primary storage location so as not to be susceptible to a common hazard.
- Configuring the alternate storage location to facilitate recovery of operation.
- Identifying and documents potential accessibility problems to the alternate storage location in the event of a wide area disruption or disaster, and implementing explicit mitigation actions.

8.5 CDA BACKUPS

This security control consists of:

- Conducting backups of user-level and system-level information.
- Backing up CDAs at an interval identified for the CDA or based on trigger events.
- Protecting backup information at the storage location.
- Testing and documenting backup information at an interval identified in the licensee's procedures and justification is provided for the interval according to the licensee's assessment to verify media reliability and information integrity.
- Using backup information in the restoration of CDAs functions as part of contingency plan testing.
- Protecting system backup information from unauthorized modification.
- Storing backup copies of the operating system and other critical CDA software in a separate facility or in a fire-rated container that is not co-located with the operational software.
- Establishing and documenting the timeframe in which data or the CDA must be restored and the frequency at which critical data and configurations are changing.

8.6 RECOVERY AND RECONSTITUTION

Mechanisms are employed with supporting procedures that allow CDAs to be recovered and reconstituted to a known secure state following a disruption or failure, and when initiated by authorized personnel. Regression testing is performed before returning to normal operations to ensure that CDAs are performing correctly.

9 TRAINING

9.1 CYBER SECURITY AWARENESS AND TRAINING

The training requirements necessary for licensee/applicant personnel and contractors to perform their assigned duties and responsibilities in implementing the requirements of the Program are established, implemented, and documented.

Individuals are trained to a level of cyber security knowledge appropriate to their assigned responsibilities in order to provide high assurance that these individuals are able to perform their job functions properly.

9.2 AWARENESS TRAINING

Cyber Security Awareness training is designed to increase an individual's sensitivity to cyber threats and vulnerabilities, and their recognition of the need to protect data information. Policy level awareness training provides employees and contractors the ability to understand security policies so that the Program is implemented. Individual users must understand their responsibility for adherence of applicable policies and standards.

Requirements are established, implemented, and documented for:

- Training programs that provide basic cyber security awareness training for facility personnel. Refresher or ongoing training provides updates on new threats and technology;
- Cyber Security awareness is provided by displaying posters, offering security-messaged items, generating email advisories/notices, and displaying logon screen messages;
- Training to include practical exercises to simulate actual cyber incidents.

The content of cyber security training is developed and documented based on the following:

- Assigned roles and responsibilities,
- The specific requirements identified by the defensive strategy, and
- The CDAs to which personnel have authorized access.

The awareness training program establishes implements and documents requirements to provide Cyber security awareness training for the appropriate employees and contractors. Awareness training addresses the following:

- The site-specific objectives, management expectations, programmatic authority, roles and responsibilities, policies, procedures and consequences for non-compliance with the cyber security program;
- General attack methodologies, including social engineering techniques; appropriate and inappropriate cyber security practices;
- Attack indicators such as:
  - Unusually heavy network traffic
  - Out of disk space or significantly reduced free disk space
  - Unusually high CPU usage
  - Creation of new user accounts
  - Attempted or actual use of administrator-level accounts
  - Locked-out accounts
  - Account in-use when the user is not at work
  - Cleared log files
  - Full log files with unusually large number of events
  - Antivirus or IDS alerts
  - Disabled antivirus software and other security controls
  - Unexpected patch changes
  - Machines connecting to outside IP addresses
  - Requests for information about the system (social engineering attempts)
  - Unexpected changes in configuration settings

  - Unexpected system shutdown
  - Unusual activity from control devices
  - Loss of signal from control devices
  - Unusual equipment in secure areas
- Organizational contacts to whom to report suspicious activity, incidents and violations of cyber security policies, procedures, or practices;
- Why access and control methods are required;
- Measures users can employ to reduce risks;
- The impact on the organization if the control methods are not incorporated.

9.3 TECHNICAL TRAINING

Training programs are established, implemented, and documented for personnel performing, verifying, or managing activities within the scope of the Program to assure that suitable proficiency is achieved and maintained. Individuals that have cyber security responsibilities related to programs, processes, procedures, or individuals that are involved in the design, modification, and maintenance of CDAs, will receive technical training.

This security control further consists of establishing, implementing and documenting requirements to:

- Provide cyber security-related technical training to individuals:
  - Before authorizing access to CDAs or performing assigned duties, and
  - When required by policy or procedure changes and plant modifications, and
  - Every 12 months, to mitigate risk and to ensure personnel maintain competency.
- Provide cyber security-related technical training on applicable cyber security concepts and practices to those individuals whose roles and responsibilities involve designing, installing, operating, maintaining, or administering (e.g., serving as a system administrator) CDAs or associated networks. Technical training addresses the following:
  - Knowledge of specific cyber security and engineering procedures, practices, and technologies, including implementation methods and design requirements, which apply to the assets they may encounter as part of their job; and
  - General information on cyber vulnerabilities, potential consequences to CDAs and networks of successful cyber attacks, and cyber security risk reduction methods.

System managers, cyber security specialists, system owners, network administrators, and other personnel having access to system-level software are provided security-related technical training to perform their assigned duties.

9.4 SPECIALIZED CYBER SECURITY TRAINING

Individuals who have programmatic and procedural cyber security authority and require the necessary skills and knowledge to execute capabilities expected of a cyber security specialist receive specialized cyber security training in order to design, execute, and manage the cyber defensive strategy effectively.

Requirements for advanced training are established, implemented and documented for individuals who are designated security experts or specialists, including the cyber security specialists with roles and responsibilities for cyber security, incident response, and the execution and management of defense-in-depth protective strategies. Advanced training addresses the following:

- Achievement and maintenance of the necessary up-to-date skills and knowledge in core competencies of data security, operation system security, application security, network security, security controls, intrusion analysis, incident management and response, digital forensics, penetration testing, and plant system functionality and operations;
- Competency in the use of tools and techniques to physically and logically harden CDAs and networks to reduce vulnerabilities to cyber attack;
- Providing cyber security guidance, assistance, and training for other staff members;
- Reviewing programmatic and system-specific cyber security plans and practices;
- Assessing CDAs, networks and assets for compliance with cyber security policies; and
- Designing, acquiring, installing, operating, maintaining, or administering security controls.

9.5 SITUATION AWARENESS

Situational Awareness training includes the normal behavior of the CDA so that abnormal behavior is recognized.

9.6 FEEDBACK

A feedback process for personnel and contractors to refine the cyber security program and address identified training gaps is established, implemented and documented. Training topics may be modified, added, or deleted as a result of this feedback

9.7 SECURITY TRAINING RECORDS

Individual cyber security training is documented and monitored.

9.8 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Contact with selected security groups is maintained to remain informed of newly-recommended security practices, techniques and technologies, and to share current security-related information including threats, vulnerabilities, and incidents. Training topics may be modified, added, or deleted as a result of these discussions.

10 CONFIGURATION MANAGEMENT

10.1 CONFIGURATION MANAGEMENT

This security control establishes, implements and documents configuration management security controls for CDAs consistent with the process described in Section 4.2 of Cyber Security Plan.

10.2 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates a formal, documented, configuration management policy, and implementing procedures that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among entities as warranted, associated configuration management controls, and compliance.

This configuration management policy is part of the site configuration management plan and includes hardware configurations, software configurations, and access permissions. Changes to hardware or software are documented and accessed in accordance with these policies and implementing procedures.

The configuration management process evaluates and controls changes to CDAs to ensure that CDAs remains secure. Confirmation that new vulnerabilities are not introduced occurs prior to any change being implemented

10.3 BASELINE CONFIGURATION

This security control develops, documents, and maintains a current baseline configuration of CDAs and their connections. As a part of the configuration management process, employs manual or automated mechanisms to maintain an up-to-date, complete, accurate, and readily-available baseline configuration of CDAs. The up-to-date baseline configurations are documented and the configurations are audited quarterly.

Baseline configuration documentation includes the following:

- A list of components (for example, hardware and software),
- Interface characteristics,
- Security requirements and the nature of the information communicated,
- Configuration of peripherals,
- Version releases of current software, and
- Switch settings of machine components.

Documentation management for baseline configurations includes:

- A log of configuration changes made,
- The name of the person who implemented the change,
- The date of the change,
- The purpose of the change, and
- Observations made during the course of the change.

A baseline configuration for development and test environments that is managed separately from the operational baseline configuration is documented and maintained. A “deny-all, permit-by-exception” authorization policy to identify and authorize software permitted on CDAs (i.e., white

lists of authorized software) is employed. After authorized changes are implemented, security features are verified to still function and cyber security levels are maintained.

Individuals authorized to modify CDA configurations are trained and qualified to perform the modifications. The minimum physical and logical access for the modifications is defined. Additionally, electronic means to monitor CDA access are employed to ensure that authorized systems and services are used. Further, the justification for the use of alternate (compensating) security controls where monitoring cannot be done electronically is documented. Justifications include:

- Physically restricting access,
- Monitoring and recording physical access to enable timely detection and response to intrusions,
- Employing auditing/validation measures (e.g., security officer rounds, periodic monitoring of tamper seals),
- Ensuring authorized individuals are trustworthy and reliable per 10 CFR 73.56,
- Ensuring that authorized individuals are operating under established work management controls, and
- Conducting post maintenance testing to validate that changes are implemented correctly.

Log records are reviewed at least quarterly, or as required by the Physical Security Plan.

10.4 CONFIGURATION CHANGE CONTROL

This security control:

- Authorizes and documents changes to CDAs.
- Retains and reviews records of CDA configuration changes and audit activities associated with CDA configuration changes.
- Employs mechanisms to:
  - Document changes to CDAs.
  - Notify designated approval authorities.
  - Prohibit implementation of changes until designated approvals are received and documented.

10.5 SECURITY IMPACT ANALYSIS

A security impact analysis is performed prior to making changes to CDAs consistent with the process described in the Cyber Security Plan to manage the cyber risk resulting from the changes. Any identified safety and security interdependencies are evaluated, documented, and incorporated into the security impact analysis.

The security impact assessment is performed and documented as part of the change approval process.

10.6 ACCESS RESTRICTIONS FOR CHANGE

The security control:

- Defines, documents, approves, and enforces physical and logical access restrictions associated with changes to CDAs and generates, retains, and audits the record quarterly, and when there are indications that unauthorized changes may have occurred.
- Implements the corrective action program to address discovered deviations.
- Employs automated mechanisms to detect unauthorized changes, to enforce access restrictions and to support subsequent audits of enforcement actions.
- Documents the justification and details for alternate (compensating) security controls where a CDA cannot support the use of automated mechanisms to enforce access restrictions, and to support subsequent audits of enforcement actions, including the following:
  - Physically restricting access,
  - Monitoring and recording physical access to enable timely detection and response to intrusions,
  - Employing auditing/validation measures (e.g., security officer rounds, periodic monitoring of tamper seals),
  - Ensuring authorized individuals are trustworthy and reliable per 10 CFR 73.56,
  - Ensuring that authorized individuals are operating under established work management controls, and
  - Conducting post maintenance testing to validate that changes are implemented correctly.

10.7 CONFIGURATION SETTINGS

This security control applies to configuration settings for CDAs by:

- Documenting the most restrictive mode,
- Evaluating operational requirements, and
- Enforcing and documenting the most restrictive operational configuration settings based upon explicit operational requirements.

This is achieved by:

- Establishing and documenting configuration settings for CDAs that reflect the most restrictive mode.
- Documenting and approving any exceptions from the most restrictive mode configuration settings for individual components within CDAs based upon explicit operational requirements.
- Enforcing the configuration settings in CDAs.
- Monitoring and controlling changes to the configuration settings in accordance with policies and procedures.
- Documenting and employing automated mechanisms to centrally manage, apply, and verify configuration settings.
- Documenting and employing automated mechanisms or manual mechanisms to respond to unauthorized changes to configuration settings.
- Documenting the justification for alternate (compensating) security controls where a CDA cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, including the following:

- Physically restricting access,
- Monitoring and recording physical access to enable timely detection and response to intrusions,
- Employing auditing/validation measures (e.g., security officer rounds, periodic monitoring of tamper seals),
- Ensuring authorized individuals are trustworthy and reliable per 10 CFR 73.56,
- Ensuring that authorized individuals are operating under established work management controls, and
- Conducting post maintenance testing to validate that changes are implemented correctly.

10.8 LEAST FUNCTIONALITY

This security control configures and documents CDA configuration settings to provide essential capabilities and prohibits, protects and restricts the use of insecure functions, ports, protocols and services.

CDAs are reviewed every 31 days to identify and eliminate unnecessary functions, ports, protocols, and services.

Automated mechanisms are documented and employed to prevent program execution. White-lists, black-lists, gray-lists application control technologies are utilized.

10.9 COMPONENT INVENTORY

This security control develops, documents, and maintains an inventory of the components of CDAs that:

- Reflect the current system configuration.
- Location (logical and physical) of components is consistent with the authorized boundary of the CDA.
- Provide the proper level of granularity deemed necessary for tracking and reporting; and deemed necessary to achieve effective property accountability.
- Update the inventory of system components as an integral part of component installations and system updates.
- Employ mechanisms to maintain an up-to-date, complete, accurate, and readily-available inventory of system components.
- Employ automated mechanisms to detect the addition of unauthorized components/devices into the environment; and disable access by such components/devices or notifies designated officials.
- Site licensee documents, the names or roles of the individuals responsible for administering those components.

11 SYSTEM AND SERVICES ACQUISITION

11.1 System and Services Acquisition Policy and Procedures

This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, system and services acquisition policy that addresses the following:
  - The purpose of the security program as it relates to protecting the organization's personnel and assets;
  - The scope of the security program as it applies to the organizational staff and third-party contractors;
  - The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments;
- A formal, documented procedure to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

11.2 Supply Chain Protection

This security control protects against supply chain threats by employing the following measures to protect against supply chain threats and to maintain the integrity of the CDAs that are acquired:

- Establishment of trusted distribution paths,
- Validation of vendors, and
- Requirement of tamper proof products or tamper evident seals on acquired products.

11.3 Trustworthiness

This security control requires that CDAs meet defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

11.4 Integration of Security Capabilities

This security control documents and implements a program to ensure that new acquisitions incorporate security controls based on the following:

- Being cognizant of evolving cyber security threats and vulnerabilities;
- Being cognizant of advancements in cyber security protective strategies and security controls; and
- Conducting analyses of the effects advancements could have on the security, safety and operation of the nuclear critical assets, systems, CDAs and networks at their facility.

11.5 DEVELOPER SECURITY TESTING

This security control requires system developers/integrators of acquired CDAs create a security test and evaluation plan, implement the plan, and document the results such that:

- The products are delivered to meet specified security requirements, and
- The delivered product is free from known testable vulnerabilities and known malicious code.

This security control also requires the plan and results be reviewed and approved by the licensee.

11.6 LICENSEE TESTING

This security control:

- Requires testing (e.g., off-line on a comparable CDA) of security devices and software to ensure that they do not compromise the CDA or interconnected CDAs operation prior to installation, and
- Deploys security controls and flaw remediation measures based on reliable and credible sources of risk information.

This security control also requires audits of CDAs, to provide high level of assurance that the safety, security, and emergency preparedness function are protected from a cyber attack to validate the following items:

- Security controls present during system validation testing are still installed and operating in the production system,
- CDAs are free from known security compromises and continue to provide information on the nature and extent of compromises should they occur, and
- Management of change program is being followed with an audit trail of reviews and approvals for changes.

12 EVALUATE AND MANAGE CYBER RISK

Risks are managed through evaluation of threats and vulnerabilities to computer and control systems during the upgrades as documented in the plant process (e.g., Engineering Design Control, Configuration Management, Software Quality Assurance, Operating Experience, and Corrective Action Program). The Program establishes in procedures or other plant documents how responses to threat notifications and vulnerabilities against a CDA received from a credible source are screened, evaluated, and adjusted.

> **NOTE:** Ensure that Safety, Security and Emergency Preparedness functions are not adversely impacted by the vulnerability scanning process. CDAs may be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If a CDA is taken off-line for scanning, scans are scheduled to occur during planned CDA outages whenever possible. When vulnerability scanning on a production CDA cannot be performed due to adverse impact on safety, security or emergency preparedness functions, alternate controls including providing a replicated system to conduct scanning, are employed.

This security control consists of establishing, implementing and documenting requirements to evaluate and address the following:

- Screen for applicability CDA vulnerability notices no less frequently than every 92 days, and at random intervals, and as necessary when new vulnerabilities affecting the CDAs are identified and reported.

For CDA Vulnerability Assessments:

- Ensure configuration information used to identify applicable cyber threats and vulnerabilities is accurate and updated when new CDAs are installed and placed into production.
- Ensure applicable threat and vulnerability information for CDAs is entered into the licensee Corrective Action Program (CAP) and evaluated in accordance with the fleet/site process.
- Ensure identified corrective actions required to mitigate threat vectors associated with applicable threat and vulnerability notifications and maintain adequate defense-in-depth are documented and tracked in CAP.

For CDA Vulnerability Scans, licensees should perform the following activities to the extent possible:

- Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting and making transparent, checklists and test procedures; and
  - Measuring vulnerability impact.
- Analyze vulnerability scan reports and remediates legitimate vulnerabilities and organizational assessment of risk; and
- Share information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.
- Employ vulnerability scanning tools that include the capability to update the list of cyber vulnerabilities scanned and updates the list of information system vulnerabilities scanned at a maximum frequency as defined in the risk determination or as necessary when new vulnerabilities are identified and reported.
- Attempt to discern what information about the information system is discoverable by adversaries.
- Perform security testing to determine the level of difficulty in circumventing the security controls of the CDAs. Testing methods may include: penetration testing, malicious user testing, and independent verification and validation (IV&V).
- Include privileged access authorization to CDAs for selected vulnerability scanning activities to facilitate more thorough scanning.
- Employ automated mechanisms to detect the presence of unauthorized software on CDAs and notifies authorized personnel.
- Review of historic audit logs to determine if a vulnerability identified in the CDA has been previously exploited.

ADDENDUM 2: CYBER ATTACK DETECTION, RESPONSE AND ELIMINATION

1 INTRODUCTION

1.1 BACKGROUND

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

10 CFR 73.54 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan. Additionally, 10 CFR 73.54(e) requires that the cyber security plan must describe how the licensee will:

i. Maintain the capability for timely detection and response to cyber attacks;
ii. Mitigate the consequences of cyber attacks;
iii. Correct exploited vulnerabilities; and
iv. Restore affected systems, networks, and/or equipment affected by cyber attacks.

Further, 10 CFR 73.54(c)(4) requires the cyber security program be designed to ensure that the functions of protected assets are not adversely impacted due to cyber attacks.

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," provides a template for the implementation of the cyber security plan. NEI 08-09, Section 2.2, discusses that the performance based requirements demonstrated in the Cyber Security Plan (CSP) that are designed to: (Section 2.2.13) Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1.

The guidance in this Addendum is applicable to any CDA. Where licensees may have used the guidance in NEI 13-10, "Cyber Security Control Assessments," the assessment elements in this Addendum would apply to Direct CDAs. Indirect CDAs have been previously assessed, in accordance with NEI 13-10, to justify the ability to detect and mitigate compromise prior to adverse impact.

Lessons learned through licensee implementation efforts, and through a series of implementation workshops conducted during 2016 that included industry and NRC observers indicate that clarification regarding the acceptable approaches to implement detection, response, and recovery elements of the Rule and CSP are warranted. The clarifications are needed to enhance clarity and consistency in implementation, and to support NRC oversight activities.

The changes in this Addendum are consistent with the cyber security program performance objective to provide high assurance that digital computer and communications systems and

networks are adequately protected against the design basis threat of radiological sabotage cyber attack as described in 10 CFR 73.1. The changes in this Addendum are intended to add necessary clarity without decreasing the effectiveness of cyber security plans implemented using the guidance in NEI 08-09.

1.2 PURPOSE

This addendum provides approaches to implement the cyber attack detection, response, and recovery elements of the Rule and CSP. This addendum intends to enhance clarity and consistency in implementation, and to support NRC oversight activities.

1.3 SCOPE

The guidance in this addendum is applicable to power reactor licensees with Cyber Security Plans (CSP) based on the template in NEI 08-09. The guidance in this Addendum is applicable to any CDA. Where licensees may have used the guidance in NEI 13-10, "Cyber Security Control Assessments," the assessment elements of this Addendum would apply to Direct CDAs. Indirect CDAs have been previously assessed, in accordance with NEI 13-10, to justify the ability to detect and mitigate compromise prior to adverse impact.

Section 2 provides a method to assess detection, response and elimination (i.e., mitigation or prevention) capabilities. Section 3 discusses the use of programs and processes for detection. Section 4 discusses the use of security operations centers, intrusion detection, and security information and event monitoring systems. Section 5 provides a series of examples consistent with the guidance in this document. The examples are intended to illustrate the level of detail appropriate for conducting an assessment of detection, response and elimination capabilities.

1.4 USE OF THIS DOCUMENT

This document may be used to implement the cyber attack detection, response, and recovery elements of the Rule and CSP for Direct CDAs. Where NEI 13-10 was used, Indirect CDAs would have been analyzed separately to determinate that any mal-operation can be detected and mitigated prior to adverse impact to SSEP functions

This document discusses the capability to detect, respond-to, and eliminate cyber attacks. In this context, the term 'eliminate' is inclusive of concepts of mitigation and prevention of the adverse impacts of a cyber attack.

1.5 ACRONYMS

The following acronyms are used in this document:

BIOS – Basic Input/Output System
CAP – Corrective Action Program
CD/DVD – Compact Disk/Digital Video Disk
CDA – Critical Digital Asset
CPU – Central Processing Unit
CSP – Cyber Security Plan

DCS – Distributed Control System
DRE – Cyber attack detection, response and elimination
HIDS – Host Intrusion Detection System
HMI – Human Machine Interface
I&C – Instrumentation & Control
I/O – Input/Output
IAW – In Accordance With
IDS – Intrusion Detection System
LAN – Local Area Network
MTE – Maintenance & Test Equipment
NIDS – Network Intrusion Detection System
OCA – Owner Controlled Area
PA – Protected Area
PC – Personal Computer
PLC – Programmable Logic Controller
PMD – Portable Mobile Device
QA – Quality Assurance
ROM – Read Only Memory
SIEM – Security Information and Event Management
SOC – Security Operations Center
SSEP – Safety-related and important-to safety functions, Security functions, and Emergency Preparedness functions including offsite communications
TCP/IP – Transmission Control Protocol/Internet Protocol
USB – Universal Serial Bus
VA – Vital Area

1.6 DEFINITIONS

The following terms are used in this document. Definitions for these terms can be found in Appendix B, "Definitions" to NEI 08-09, Revision 7, and are not reproduced here:

- **Commercial Off-The-Shelf (COTS) Software**
- **Custom Software**

2 DETERMINATION OF DETECTION, RESPONSE AND ELIMINATION CAPABILITIES

2.1 TIMELY ATTACK DETECTION

Timely detection can be demonstrated through the use of near real time automated capabilities, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway. One example of detection along an attack pathway is supply chain testing which includes anti-virus scanning and verification of proper equipment operation (i.e., detection for anomalous behavior).

When considering the timeliness of detection capabilities, a basis may be developed which is consistent with other evaluated and approved outage or compensatory time (e.g., technical specifications, physical security plan). When considering if a licensee has timely detection, the following questions should be asked:

1) Did the licensee place its detection capability along the attack pathway(s) at a location where it can detect cyber attacks and permit the licensee to respond and eliminate the cyber attacks before an adverse impact to the SSEP function?
2) Are personnel responsible for cyber attack detection trained in accordance with licensee training standards, and are they sensitive to the indications of a cyber attack?

2.2 ADEQUATE DETECTION

Does the licensee have the ability to:

1) Timely detect and respond to malicious activity utilizing:
   a) Known features or signatures (signature based); or
   b) Known anomaly or indicators (anomaly based) detection (automated if technically possible and manual if not).
2) Determine the cause of the security event (i.e., that it is cyber security related); and,
3) Mitigate or eliminate the threat using documented processes and strategies?

Information to consider when determining adequate detection:

1) Adequacy of detection:
   a) Are responders trained in accordance with licensee training standards on detection indicators?
   b) Does the licensee use whitelisting if technically possible?
2) Adequacy of signature based detection:
   a) If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators as required.
3) Adequacy of anomaly based detection:
   a) Does the licensee use anomaly detection indicators as part of its detection strategy and update the anomaly indicators as required.
4) Integrity of the Intrusion Detection System (IDS):
   a) If automatic IDS is used, is the IDS capable of detecting and preventing unauthorized changes to itself?

2.3 TIMELY ADEQUATE RESPONSE AND ELIMINATION

Response

Does the licensee have the ability to respond in a timely fashion to a cyber attack and eliminate the threat and prevent adverse impact to the SSEP function?

Information to consider when determining response ability:

1) Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on-site or on-call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber attack.
2) Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?

Information to consider when determining adequacy of personnel response:

1) Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?
2) Are procedures exercised and tested?
3) Is the equipment the personnel use for response available to them?
4) Is the environment the personnel respond adequate (environmental considerations addressed) to successful response?

Cyber Attack Elimination and Prevention of Adverse Impact to the SSEP Function

Does the licensee have the capability to use existing equipment or actions which prevents, eliminates or mitigates the adverse impact to SSEP function?

Information to consider when determining the adequacy of response and elimination of a cyber attack:

1) Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS/CDA?
2) Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?

3 DETECTION USING PROGRAMS AND PROCESSES

Timely detection can be demonstrated through the use of near real time automated capabilities, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway.

Where technological methods for detection are not implemented, alternate methods (as described in Section 3.1.6 of the CSP) may be considered and implemented. When crediting alternate methods for detection, licensees should evaluate the methods and ensure they provide an adequate level of timely detection and timely response in order to prevent adverse impacts to the required functions (the goal is to ensure that the functions of protected assets identified by 10 CFR 73.54(b)(1) are not adversely impacted due to cyber attacks, not necessarily mal-operation of an individual CDA). The basis for crediting the alternate program should be incorporated into licensee documentation and sufficiently justified to withstand regulatory scrutiny.

Examples of programs and processes that may form the basis for alternate controls for detection include, but are not limited to:

- Operations rounds / operations monitoring
- Plant maintenance activities / troubleshooting procedures
- Plant modification testing / return to service testing
- System trouble alarms (annunciators) / plant computer alarms
- System engineering performance and condition monitoring software

For digital components not capable of advanced detection methods that were installed and operational prior to the full implementation of the CSP requirements, plant operating history and normal plant testing at the time of installation is sufficient to establish a baseline for anomaly detection for these devices.

3.1 USE OF SECURITY (IMP) OR OTHER ROUTINE ROUNDS FOR DETECTION

Where the licensee relies on Insider Mitigation Program (IMP) patrols or other routine rounds or surveillances to detect attempts to bypass access controls to a CS/CDA, the licensee ensures that the individuals are trained to recognize obvious indications of cyber tampering.

1) In the case of the CDA being located within the VA, the access monitoring and control mechanisms, site security program IMP rounds and 24/7 staffing of the control room provide an acceptable level of unauthorized physical access detection. Also, when CS\CDA maintenance is being performed, normal plant maintenance actions require verification by a technically knowledgeable individual to ensure proper completion of work orders and a closeout inspection of any collocated CDAs for evidence of tampering.
2) In the case of the CDA being located within the PA (but not the VA) then the licensee should consider additional controls for Direct CDAs or CDAs associated with the proper operation of Vital Equipment. In these cases, the use of physical tamper prevention and detection mechanisms (e.g. serialized tamper tape, port lock/blocking devices, locking enclosures, locking covers, or other positive means of detection, etc.), would provide an acceptable means for detecting unauthorized physical access and detection. Also, when

CS\CDA maintenance is being performed, normal maintenance actions require verification by a technically knowledgeable individual to ensure proper fulfilment of work orders and a closeout inspection of any collocated CDAs for evidence of tampering.

3.2 USE OF SYSTEM AND SERVICES ACQUISITION CONTROLS FOR DETECTION

The cyber security controls in NEI 08-09, Appendix E, Section 11, "System and Services Acquisition," can provide means for detecting cyber attacks. Addendum 3, "System and Services Acquisition," to NEI 08-09, Revision 7, provides guidance related to the implementation of the NEI 08-09, Appendix E.11 cyber security controls.

Licensees may refer to the following sections of the Addendum 3 guidance for methods that can be used for cyber attack detection:

- Section 2.1.2, "Maintaining Custody and Control of Devices or Software from a Vendor to Installation;" and,
- Section 2.2.6, "Appendix E.11.6, Licensee Testing."

4 USE OF OPERATION CENTERS AND CENTRALIZED DETECTION

4.1 USE OF A SECURITY OPERATIONS CENTER (SOC)

Licensee may utilize a Security Operations Center (SOC) as a component of their detection, monitoring and response implementation. The use of the SOC should be documented and incorporated as a component of the licensee's procedures and processes. The information and logs sent to the SOC should be evaluated against existing licensee procedures for security sensitive information protection and records retention to ensure that appropriate requirements are implemented. Where necessary, based on the classification of the information, the licensee should provide technical methods to protect information in transit and at rest in accordance with licensee procedures.

Where SOC services utilized are provided by a third party (including a non-nuclear entity within a utility), a Service Level Agreement (SLA) or similar document should be established to outline the roles and responsibilities of all groups involved. The SLA should also outline the lines of demarcation between the licensee and the service provider.

It is not anticipated that personnel at a corporate or third party SOC have access, extensive knowledge, or administrative control over plant digital computer and communication systems that warrant inclusion in the "critical group" as described in 10 CFR 73.56.

4.2 DELAY IN IMPLEMENTATION OF INTRUSION DETECTION OR SECURITY INFORMATION AND EVENT MONITORING (SIEM) SYSTEMS

This section provides guidance for crediting alternate methods of cyber attack detection where a planned Intrusion Detection System (IDS) or Security Information and Event Management (SIEM) system installation cannot be completed prior to the full program implementation date. The guidance in this section should be considered in cases where the licensee cannot implement alternative controls for detection described in the other sections of this document.

In the case where the licensee has planned to implement an IDS on a **safety system** (and this activity is recorded in their CAP) but this has not been accomplished by the full implementation date due to the need for a scheduled outage, the licensee must show that required changes could not be accomplished without an outage. (Note: installing a NIDS may not require taking a system down/out-of-service to accomplish its installation but implementing a HIDS does.) The licensee shall implement the alternate security measures below to provide the ability to detect a cyber compromise before adverse impact to the SSEP function. The following actions would be considered adequate alternate security controls, provided the completion of the corrective action and IDS installation is completed within sixty days (to permit adequate close out of the change package) of the last day of the outage.

In the case where the licensee has planned to implement an IDS on a **security system** (and this activity is recorded in their CAP) but this has not been accomplished by the full implementation date, the licensee must show that required changes could not be accomplished without a delay beyond the full implementation date. (Note: installing a NIDS may not require taking a system down/out-of-service to accomplish its installation but implementing a HIDS does.) The licensee

shall implement the alternate security measures below to provide the ability to detect a cyber compromise before adverse impact to the SSEP function. The following actions would be considered adequate alternate security controls, provided the completion of the corrective action and IDS installation is completed within six months of the full implementation date.

Alternate measures for monitoring until installation of the planned IDS:

If the CS/CDA is located within the **Vital Area**:

1) The CS/CDA is monitored by IMP patrols and/or continually manned by personnel in the critical group;
2) The CS/CDA audit/logging functionality, if technically supported, is implemented and enabled and the logs extracted, reviewed and a report on the contents generated, at least once a month;
3) The CDAs performance is tested or verified against a secondary or alternate indicator weekly and when required to make operational decisions;
4) The CS/CDA is isolated with no communication pathways to other systems. If the CS/CDA communicates with other systems/devices then those systems/devices meet the same criteria as described above in 1 through 3;
5) The licensee's PMMD program has been inspected and found to be adequate; and,
6) The licensee installs a non-disclosed (i.e., not prescribed here) method of timely detection on the system.

If the CS/CDA is located within the **Protected Area** but outside the VA:

1) The CS/CDA audit/logging functionality, if technically supported, is implemented and enabled and the logs extracted, reviewed and a report on the contents generated, at least once a month;
2) The CS/CDA performance is tested or verified against a secondary or alternate indicator weekly and when required to make operational decisions;
3) Visible tamper indicators are used, surveyed and documented by plant personnel once every 24 hours and/or the CS/CDA is within a locked and alarmed enclosure or monitored by continuous video surveillance;
4) The CS/CDA is isolated with no communication pathways to other systems. If the CS\CDA communicates with other systems/devices then those systems/devices meet the same criteria as described above in 1 through 3;
5) The licensee's PMMD program has been inspected and found to be adequate; and,
6) The licensee installs a non-disclosed (i.e., not prescribed here) method of timely detection on the system.

If the CS/CDA is located **outside the PA**:

1) The CS/CDAs are located in areas that meet the requirements of NEI 08-09, Appendix E, Section 5;
2) The CS/CDA audit/logging functionality, if technically supported, is implemented and enabled and the logs extracted, reviewed and a report on the contents generated, at least once a month;
3) The CS/CDA performance is tested or verified against a secondary or alternate indicator weekly and when required to make operational decisions;

4) Communication pathways into the CS/CDA (including the communication media) are physically secured against tampering and surveyed weekly, and the other systems/devices with which the CS/CDA communicates meet the same criteria as described above in 1 through 3;
5) The licensee's PMMD program has been inspected and found to be adequate; and,
6) The licensee installs a non-disclosed (i.e., not prescribed here) method of timely detection on the system.

5 DETECTION, RESPONSE AND ELIMINATION EXAMPLES

Below are examples of various components and systems, and acceptable ways to answer affirmatively the DRE filter questions provided in Section 2. In accordance with Section 3.1.6 of the CSP, alternate controls/countermeasures may be implemented that eliminate threat/attack vector(s) associated with one or more of the cyber security controls. These can be employed by performing an analysis and documenting the basis for implementing an alternative countermeasure which provides cyber security protection commensurate with the corresponding cyber security control.

The examples in this section below do not provide detailed information about system architecture nor processes, but does include alternate controls and standards that are acceptable for detection and response.

5.1 EXAMPLE 1: STANDARD COMPUTER SYSTEM

This computer system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The system has many connections and nodes,
- The system is running Microsoft Windows operating system, and
- The system supports fully functioning NIDS and HIDS.
- This computer system is isolated with no other connectivity.
- The attack pathways into this system are by way of USB drives, CD/DVD drives, wireless networks, and vendor MTE laptops.
- The licensee has an effective and adequate PMD protection program, which prevents known malware infected USB drives and CD/DVD from accessing the system.

Where along the attack pathway will the licensee detect a cyber attack?

Detection along the threat pathway includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable Media__X__

IDS (HIDS/NIDS) __X_

Access Control____

Wireless_X__

Operator __X___

IMP__X__

The "X"ed items are potential areas that can used to detect a cyber intrusion along the threat pathway. The pathway includes supply chain, portable media devices, wireless networks, and HMIs.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	HIDS/NIDS has been installed and implemented in threat attack pathway to detect cyber attack.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are training IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	The system uses whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates signature indicators as required.
Adequacy of anomaly based detection		

Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	HIDS/NIDS is protected with anomaly detection capability.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	HIDS/NIDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses the Corporate SOC as the 24/7 basis as well as onsite monitoring and response.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee onsite CSIRT and SOC personnel are appropriately trained, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive and respond to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop drills and exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.

Is the environment the personnel respond to adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee training standards.

5.2 EXAMPLE 2: COMPUTER SYSTEM EXAMPLE A

System description

- Computer System is being upgraded as part of the full implementation cyber security program implementation and to address equipment obsolescence. The computer system is not safety-related but it provides an SSEP function.
- The Computer System includes a lot of connections to field devices. Outside of the field devices, which are part of the overall SSEP system, no other connections are provided to other systems so the Computer System is air gapped from any other plant systems, in Level 4 of the defensive architecture.
- Upgraded system is designed to be cyber security compliant with the cyber security plan. An intrusion detection system (IDS) function, intrusion prevention system (IPS) function and security information and event management (SIEM) function will be included in the upgraded system.
- Whitelisting will be built in to the upgraded system.
- No wireless capabilities are included in the Computer System.
- Equipment cabinet access controlled through the key control program and work management processes.
- Equipment cabinets contain alarm connections which result in alarm when opened.
- PMMD program used to ensure secure connections with removable media.
- Cyber testing performed during Factory Acceptance Testing and Site Acceptance Testing. Software controls included in the vendor activities for software requirement development, software design, software testing, and software V&V. Vendor has cyber security program and testing capabilities.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	SIEM, HIDS/NIDS, IPS has been installed and implemented in threat attack pathway to detect cyber attack. PMD control program will detect known malware on portable media and devices.

		System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured. The cabinets are in vital area and access control notifications alarmed and a location staffed 24/7.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	The system uses whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates signature indicators as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	HIDS/NIDS performs anomaly detection capability and updates indicators as required.
Integrity of the Intrusion Detection System		

If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	HIDS/NIDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses the Corporate SOC as the 24/7 as well as onsite duty analyst or 24/7 response onsite and CSIRT for monitoring and response. If using corporate SOC, information is protected in accordance with site information protection standards such as VPN or encryption. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee onsite and SOC personnel are appropriately trained, in accordance with training standard.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standard.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.

Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures.

5.3 EXAMPLE 3: COMPUTER SYSTEM EXAMPLE B

System Description:

- System includes servers, workstations and firmware-based components.
- System has fully functional SIEM including custom developed SIEM rules.
- Logs are centrally collected by SIEM from devices that have the ability to send logs.
- SIEM provides notification of an identified abnormal condition in near real-time.
- System does not utilize NIDS.
- Whitelisting, HIDS, data loss prevention, and antivirus software are enabled, and sends logs to the SIEM.
- Wireless capability is disabled.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	SIEM, HIDS, IPS has been installed and implemented in threat attack pathway to detect cyber attack. PMD control program will detect known malware on portable media and devices. System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured. The cabinets are in vital area and access control notifications alarmed in a location staffed 24/7.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are training in accordance with licensee training strategies and procedures.
Adequate detection:		

Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	The system uses whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates signature indicators as defined in procedures.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	SIEM has the ability to performs anomaly detection and anomaly indicators are updated as they become available.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	HIDS is configured to detect unauthorized changes to itself .
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst for monitoring and CSIRT for response and the Corporate SOC as backup. Personnel are trained to training standards.

Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee onsite are appropriately trained, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond adequate to successfully response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures.

5.4 EXAMPLE 4: VINTAGE COMPUTER SYSTEM

Background

- Not feasible to replace the current vintage Computer System prior to full program implementation date.
- Current plan is to use the current Computer System for a short time until completion of the upgrade in a date in the near future.
- New system will meet all Detection Response and Elimination control requirement
- Current Vintage Computer System attributes
- Windows Server 2003
- Open VMS Servers
- Windows XP Workstations
- Standalone Level 4 system
- Nortel Network Switches – Server / Workstation / MUX communication
- MUX Boards – Field Device signal inputs and response / Conversion to network data / Generating Fault Alarms
- All equipment in the PA, except for some field I/O equipment
- Cables in hardened conduit with intrusion monitoring on junction boxes
- Field devices - Inaccessible interface ports, fault alarms to continuously manned locations.
- Continuously manned locations with strict access control.
- Locked cabinets for servers.
- Add Port Lockers for exposed ports, with periodic monitoring. (Switches in open cabinets)
- Port Blocking on exposed equipment with periodic monitoring
- Add virus protection to Servers / Workstations with manual updates and local management.
- Increase / validate OS security event logging on Servers and Workstations.
- Manual log collection with connector to SIEM for use case alerting

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	Anti-virus is installed in the threat attack pathway on the Windows workstations to detect cyber attack. Manual log collection with a connector to a SIEM for alerting and response before adverse impact. Monitored port blocking and PMD control program will detect malware on portable media and devices. System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured. Any hardware/software changes made to the system is tested to detect anomalous behavior. The cabinets are in vital area and access control notifications alarmed and a location staffed 24/7.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not used because patching of the systems is not allowed -there is no vendor support and this attack pathway does not exist. Any changes made to the

		system are tested to detect anomalous behavior. No software changes are allowed on the system. PMMD program in place for extraction of system data and logs performed bi-weekly.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates antivirus signature indicators as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Periodic functional tests of the equipment will indicate anomalous behavior. No software changes are allowed on the system.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	AV software is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses the Corporate SOC as the 24/7 as well as onsite duty analyst and CSIRT for monitoring and response. Manual Logs are sent to SOC for evaluation bi-weekly. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and	Yes	Licensee onsite and SOC personnel are appropriately trained, in accordance with training standards.

conduct an initial response to cyber attack alarm conditions?		
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures.

5.5 EXAMPLE 5: DIGITAL DISTRIBUTED CONTROL SYSTEM EXAMPLE A

This control system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The digital distributed control system uses a multi-channel, "voting" scheme based on PLC technology that incorporates microprocessors to execute the monitoring and protection logic.
- These devices are "programmable"; definition of the logic functions are user configurable and alterable in the field with the use of the vendor's configuration software tools.
- Basic firmware that interprets and executes the user-defined logic burned in ROM and not field-alterable or upgradable.
- A PC workstation running Microsoft Windows operating system and fully functioning HIDS, is used for system configuration and a local high-speed communication interface is used to connect with the control system for configuration purposes.
- Interface is based on Ethernet-TCP/IP protocols.
- The configuration workstation is permanently connected to the SSEP system as opposed to temporarily being connected when configuration changes are required.
- USB ports.
- Control system in Level 4 behind a one-way deterministic boundary device with no bypasses.
- The licensee does not require the vendor to maintain an effective PMD program nor ensure integrity of the software and information flow which is introduced by vendor representatives.

Detection along the Attack Pathway Includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable Media__X__

IDS (HIDS/NIDS) _X__

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	Workstation HIDS. PMD control program will detect known malware on portable media and devices. System and Services Acquisition controls IAW with the CSP that ensure testing for anomalous behavior is in place that will detect malware in devices being procured.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is used.
Adequacy of signature-based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates antivirus signature indicators as required.
Adequacy of anomaly-based detection		
Does the licensee use anomaly indicators as part of its detection	Yes	Anomaly detection is used and updated as required.

strategy and update the anomaly indicators with (frequency)?		Signature and anomaly Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is capable of detecting unauthorized changes on itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in

		accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.6 EXAMPLE 6: DIGITAL DISTRIBUTED CONTROL SYSTEM EXAMPLE B

Background

- Not all components are located in the Main Control Room (MCR); the cabinets are alarmed to an annunciator in the MCR.
- The system does not contain a Microsoft Windows PC connected for normal system operations.
- Components are dedicated and not swapped between SSEP and non-SSEP systems.
- USBs are not used with this system, but laptops are controlled in accordance with the PMD program.
- System undergoes rigorous calibration and functional checks during outages and limited portions are tested while online.
- This is a Level 4 networked system; hardware design prohibits incoming connections.
- Plant Operations personnel continuously monitor plant parameters associated with this system. Abnormal operation or indication would be identified by operations personnel.
- Access to the cabinets is alarmed to the main control room, unauthorized attempts to access the equipment would be detected by indications in the MCR.
- This equipment is located in a locked and alarmed cabinet, which is monitored 24x7 by the MCR.
- Wireless functionality is not supported.
- Rogue wireless scans are performed in areas around the computer systems.
- Surveillance instructions and calibrations are performed on this equipment.
- PMD control provides adequate protection to mitigate and detect the PMD attack vector.
- Procurement of devices in accordance with System and Services Acquisition cyber security controls in the CSP would detect.
- This equipment is located in VA within locked and alarmed cabinets that have a key control program. Alarms are sent to annunciators in the MCR when cabinet doors are opened.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	The system does not contain a Microsoft Windows PC connected for normal system operations. Operations personnel continuously monitor plant parameters associated with this system. Abnormal operation or indication would be identified by operations personnel. Access to the cabinets is alarmed to the main control room; unauthorized attempts to access the equipment would be detected by indications in the MCR. USBs are not used with this system, but laptops are controlled in accordance with the PMD program and software from the vendor is screened. Detection through System and Services Acquisition testing methods is conducted for new software introduction. System undergoes rigorous calibration and functional checks during outages and limited portions are tested while online. Hardware design prohibits incoming connections. Any changes made to the system are tested to detect anomalous behavior.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber-attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		

Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible for this system. Any changes to the processor configuration or to the software will be identified during rigorous calibration and functional checks during outages and limited portions are tested while online. Operations personnel continuously monitor plant parameters associated with this system. Abnormal operation or indication would be identified by operations personnel. The cabinets are located in the Vital Are or in the PA, access to the cabinets is alarmed, and unauthorized attempts to access the equipment would be detected by indications in the main control room.
Adequacy of signature-based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection is not technically possible. See above for detection capabilities. Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Adequacy of anomaly-based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly detection is not possible, but by abnormal operation or indication would be monitored and identified by operations personnel. Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	The systems does not have an IDS capability, but abnormal operation or

		indication would be monitored and identified by operations personnel.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst for monitoring and CSIRT for response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		

Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.7 EXAMPLE 7: DIGITAL REACTOR PROTECTION SYSTEM

Background

- Digital Reactor Protection System (RPS) was upgraded in 2009-2011 due to equipment obsolescence.
- Four-channel system uses a voting scheme to determine the need to trip the control rod drive breakers to protect the reactor at predetermined trip set points. The system is safety-related and provides an SSEP function.
- Self testing and diagnostic functions provided in the system design capabilities.
- Digital RPS is located in Level 4 behind a data diode.
- Digital RPS connection to plant computer through a port tap aggregator one-way connection.
- No wireless capabilities are included in the Digital Reactor Protection System.
- Does not include HIDS or NIDS capability in the current system design.
- The system can be configured using the Monitoring and Service Interface, which is built into the system. Configuration controlled by the design change process and implemented with plant procedures.
- Monitoring and Service Interface through a Service Unit workstation located in the control room. Bi-directional connection between the Service Unit and the safety processors. The Service Unit uses a Linux operating system. The Service Unit Service unit connection is a continuous connection. Interface between the Service Unit and the safety processors is controlled by the key switch module in each cabinet.
- Key switch module controls the operation mode of the system. Key switch must be placed in change-enabled mode in order for configuration changes to be made. Key switch key is control via the key control program and the key switch module is located in the cabinet. Key switch position parameter change enable position is provided to the control room via annunciator alarm.
- A maintenance laptop is available for the system and is stored in a cabinet in the Control Room. Laptop dedicated to the Digital RPS and only includes the software needed to interface with the digital system. The laptop uses a Linux operating system. The system run time environment software is written so the laptop can only be connected when a channel is out of service because the associated connector is not recognized by the safety processor during normal processing cycles.
- Equipment cabinet access controlled through the key control program and work management processes.

- Equipment cabinets contain alarm connections which result in control room annunciator alarm when opened.
- PMMD program used to ensure secure connections with removable media.
- Cyber testing performed during Factory Acceptance Testing and Site Acceptance Testing. Software controls included in the vendor activities for software requirement development, software design, software testing, and software V&V. Vendor has a cyber security program and testing capabilities.
- Insider mitigation program used to ensure trustworthy individuals work on the system. Vendor representatives are not granted access to the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System does not support IDS, however, anomalous behavior would be detected because Monitoring and Service Interface has built in detection so that preconfigured messages, which are in the correct format and not faulted will be accepted. Faulted messages are ignored. Faulted signals are alarmed. The safety processors have self-testing and functional verifications, which are performed continuously, and any faults or deviations are alarmed. Configuration changes can only occur when the key switch module is placed in the parameter change enable mode by turning the key in the module. The key switch must be accessed by opening the cabinet, which is locked. The key for the key switch and for the cabinet is controlled by operations in the key control program. Prior to issuing the key switch key, the associated channel is placed in either bypass or trip condition. Cabinet access control notifications built into the system design such that physical

		access into the cabinets will be alarmed in the control room by annunciator. Key switch mode is alarmed when the key switch is placed in the parameter change enable mode. Channel check verification performed by operation personnel each shift. System and Services Acquisition controls IAW the CSP will test and detect any new software introduced for anomalous behavior into system
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, V&V and installation. No additional code or modification is authorized IAW with the NRC approved safety system licensing basis document.
Adequacy of signature-based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee	Yes	Signature-based detection is not technically possible on the system. See above for detection capabilities. Detection through System and Services

update the signature indicators within (frequency)?		Acquisition testing methods is conducted for new software introduction. System design results in any effort to change the code will alarm and notify operators who will take appropriate action in accordance with approved procedures.
Adequacy of anomaly-based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly detection is not possible on the system, but by system design any effort change the code will alarm and notify operators who will take appropriate action in accordance with approved procedures. Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	Detection of unauthorized changes by an IDS system is not available, but by system design any effort change the code will alarm and notify operators who will take appropriate action in accordance with approved procedures.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and	Yes	Licensee personnel are appropriately trained to assess and conduct an initial

conduct an initial response to cyber attack alarm conditions?		response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.8 EXAMPLE 8: STANDARD LEGACY COMPUTER SYSTEM (PLANT COMPUTER)

This computer system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The legacy computer system is a central data acquisition and display system that collects real-time measurements from process areas all around the plant including the numerous isolated subsystems, using a combination of analog/contact/pulse input signals and point-to-point communication connections.
- It is based on a legacy computer and networking technology.
- This system also provides real-time plant information to the NRC and, in emergency situations, to off-site emergency monitoring and response facilities setup by the licensee.
- Systems also feed plant data to separate plant historian systems.
- The connectivity to diverse subsystems usually includes communications with meteorological stations geographically dispersed around the OCA and surrounding areas.
- Includes a gateway device in the computer room to make plant data available to other systems via TCP/IP networking but the gateway device is connected to a one-way boundary device.
- The computer system has numerous serial communication channels that go out to various smart devices and subsystems around the plant and local area. These serial communication circuits are individually managed by separate application programs that use them to “poll” and receive data value updates from those devices/subsystems.
- These application programs process the in-coming messages a character at a time and will immediately reject and flush any message that does not conform to the protocol specifications. They also do not accept ad-hoc messages from those devices/systems and any such message traffic would be rejected as spurious and unsolicited.
- The protocols used incorporate message length information (and maximum allowed message sizes) and so buffer-overflows are not a consideration.
- Operators double-check critical values against multiple sources.
- For the out-going data supplied by the computer system to external systems (e.g. plant historian, NRC, off-site monitoring) this data passes through a one-way boundary device that precludes incoming information flow.
- The system has physically distributed I/O multiplexors that are used to read analog, contact and pulse signals and convert them into measurement values, which can be trended, displayed and alarm checked by application software in the servers.
- The communications between the computer and the I/O multiplexors is a proprietary message protocol. The I/O LAN is a proprietary hardware design.

- This system supports an early version of Ethernet with a legacy network (which is not TCP/IP based.)
- System supports removable media in the form of cartridge tape modules and pre-dates the development of floppy disks and USB devices.
- Communication software on this system used to communicate with "smart" devices and subsystems, was custom-developed by the system integrator and not a commercially available application.
- The operator displays in the control room are generally "dumb" terminals or slaves to operator display applications running on the central computers.
- There are Personal Computer workstations emulating the virtual functionality connected to each of the redundant computers. The computers provide both real-time plant information, including reactor optimization calculations, as well as running specialized application programs that support emergency response activities. The programs on this system are no longer supported by a vendor.

Detection along the threat pathway includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable Media__X__

IDS (HIDS/NIDS) _ _

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	To address detection, the licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and

		elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices. Access control for HMI/Keyboard, critical values checked, software changes are verified against signature and anomaly based indicators.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	System does not support whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The system does not support Signature based detection. However, System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured prior to introduction into the plant systems. PMD control program will detect malware on portable media and devices. Access control for HMI/keyboard, critical values checked, software changes are

		verified against signature and anomaly based indicators.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indication is not supported by this system. However, anomaly testing as part of the System and Services Acquisition controls are used. Also, operators monitor these systems 24/7 and will be able to detect anomalous behavior in plant equipment.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is not supported on installed equipment, but is supported in equipment used a part of supply chain and acquisition equipment used to ensure adequate testing prior to being installed in plant systems.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		

Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.9 EXAMPLE 9: LEGACY COMPUTER SYSTEM EXAMPLE A

Background

- Legacy Computer System is not safety-related but it provides an SSEP function.
- The Legacy Computer System includes a lot of connections to field devices.
- Connections to other plant systems such as control systems and monitoring systems are provided through the local area network, which is the infrastructure, built into the Legacy Computer System.
- An intrusion detection system (IDS) function and security information and event management (SIEM) function will be included in the local area network that the Legacy Computer System uses to connect to the other systems.
- Whitelisting is not included in the Legacy Computer System or the local area network infrastructure.
- No wireless capabilities are included in the Legacy Computer System.
- Equipment cabinet access controlled through the key control program and work management processes.
- PMMD program used to ensure secure connections with removable media.
- Software controls included in the vendor activities for software requirement development, software design, and software testing.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System has IDS and a SIEM, which monitors connections within the plant LAN that is the interfacing system between the plant computer and the other plant digital control and monitoring systems. Any changes to the processor configuration or to the software will be

		performed by the design change process, which includes requirements for design development (hardware and software), testing, and installation. The licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices. Access control for HMI/Keyboard, will ensure control of this equipment.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible because the system is a legacy system and is not supported anymore and the system may become unstable with whitelisting installed.
Adequacy of signature based detection		

If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection indicators are updated as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indictors are accomplished as part of the App E section 11 System and Services Acquisition program. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, and installation Detection through System and Services Acquisition testing methods is conducted for new software introduction. The IDS noted on the LAN also performs anomaly detection. Operators also monitor plant other confirmatory plant equipment 24/7 and will identify anomalous equipment behavior.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.

Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.10 EXAMPLE 10: LEGACY COMPUTER SYSTEM EXAMPLE B

Background

- Non-Windows OS with limited OEM support, and modern TCP/IP networking protocols in use.
- Configures on the CPU are such that network traffic is dropped unless ports and protocols are explicitly defined.
- Tapes are not used.
- Interfaces are licensee developed and supported.
- Satellite display terminals are Windows PCs with a GUI-based application.
- The equipment is located in the PA and VA within locked cabinets with key control, or protected with tamper seals, or located in a 24/7 manned area, or identification/authentication mechanisms (e.g. usernames/passwords) are used.
- The SIEM deployed in accordance with procedure requirements provides mechanisms to identify and notify individuals of abnormal cyber conditions on the system.
- Notifications of events identified by the SIEM are sent to the cyber security analysts for investigation. The SIEM collects logs from systems, which support log forwarding including HIDS, Anti-Virus, Rogue System Detection, and Data Loss Prevention.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	Centrally managed antivirus, whitelisting, and data loss prevention software is deployed and monitored by SIEM to detect and prevent malicious software or unauthorized PMD use. The SIEM collects logs from systems, which support log forwarding including HIDS, Anti-Virus, Rogue System Detection, and Data Loss Prevention. PMD control provides adequate protection to mitigate and detect the PMD attack vector.

		Portions of this system are located in an area manned 24/7. Personnel stationed in the area would detect signs of malicious activity. Procurement and testing of devices in accordance with System and Services Acquisition cyber security controls would detect anomalous behavior.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Centrally managed whitelisting is deployed and monitored by SIEM to detect and prevent malicious software.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection indicators are updated as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	The licensee uses anomaly indicators as part of its detection strategy and updates the anomaly indicators as needed. Personnel trained to detect abnormal operation of the equipment. Training of personnel includes their role specific

		training and role based cyber security training.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	Yes, the IDS has whitelisting installed, which would detect changes on itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee use a cyber security operations center manned and trained, in accordance with licensee training standards, personnel to assess and respond to cyber attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst and CSIRT for monitoring and response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.

Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.11 EXAMPLE 11: MICROPROCESSOR BASED I&C SYSTEM EXAMPLE A

This I&C system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The digital I&C system is a multi-functional mainframe data acquisition and control system associated with an SSEP function.
- This system is a highly functional digital system with a CPU, firmware, memory, HMI, digital and analog I/O with serial and Ethernet communications capability and the system is located in the control room.
- The chassis is designed to be modular and therefore share common components with other systems, both those associated with SSEP functions and those not associated with SSEP functions.
- This licensee strives to reduce spare parts by interchanging common parts and components thus reducing inventory requirements and cost. Therefore, the licensee uses multiple common parts and components in both SSEP and non-SSEP systems.
- Because the licensee interchanges the components and because some of the components are used in SSEP associated systems, the licensee protects all common parts for both SSEP and non-SSEP systems as CDAs such that the integrity of the components are maintained.
- The device has portable USB drives and only personnel who have been determined trustworthy in accordance with 10 CFR 73.56 and have a need for access, are granted access to the HMIs.
- Because of the limited nature of the operating system and communication protocols on this system and modules, an IDS would not be supported.
- This system is protected by and behind a one-way deterministic boundary device with no bypasses. The system modules functionality is firmware based requiring physical access and the system to be taken off line to change its functionality.

Detection along the threat pathway includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable Media__X__

IDS (HIDS/NIDS) _ _

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	The system is not capable of supporting and IDS. Software changes are tested against signature and anomaly based indicators. PMD control program will detect malware on portable media and devices. Access control for HMI/keyboard, and critical values are checked.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators .
Does the licensee use whitelisting if technically possible?	Yes	System does not support whitelisting. CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software.
Adequacy of signature based detection		

If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The system does not support IDS or AV and as a result, signature based detection is not technically possible. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software. PMD control program will detect use signature based indicators to detect malware on portable media and devices.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indication is not supported by this system. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious, anomalous behavior, and unneeded software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. Operators monitor these systems 24/7 and will be able to detect anomalous behavior in plant equipment.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is not supported on installed equipment.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response.

security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?		Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.12 EXAMPLE 12: MICROPROCESSOR BASED I&C SYSTEM EXAMPLE B

Background

- Distributed Control System (DCS) was installed to address equipment obsolescence of the Westinghouse NSSS control system. The DCS is not safety-related and it controls the operation of the secondary side plant systems for feedwater, steam generator level, etc.
- The DCS includes a lot of connections to field devices for both input to the control processes and for output to control the plant equipment response for the given power conditions.
- A network connection is provided to the plant computer to provide information to plant personnel for monitoring of the DCS and plant parameters.
- Upgraded system was designed to be cyber security compliant with the licensee cyber security program, which was developed for NEI 04-04.
- An intrusion detection system (IDS) function and security information and event management (SIEM) function was included in the DCS.
- Whitelisting was not included in to the upgraded system.
- No wireless capabilities are included in the Distributed Control System.
- Equipment cabinet access controlled through the key control program and work management processes.
- PMMD program used to ensure secure connections with removable media.
- Software controls included in the vendor activities for software requirement development, software design, and software testing. Vendor has software quality program and testing capabilities.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System has IDS and a SIEM, which monitors connections within the plant LAN that is the interfacing system between the plant computer and the other

		plant digital control and monitoring systems. Any changes to the processor configuration or to the software will be performed by the design change process, which includes requirements for design development (hardware and software), testing, and installation. The licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible. Changes to system software will require design and testing by the vendor or software developer to ensure no unexpected software code is provided with a change.

Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection indicators are updated as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indictors are accomplished as part of the App E section 11 System and Services Acquisition program. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, and installation. Operators also monitor plant other confirmatory plant equipment 24/7 and will identify anomalous equipment behavior.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is capable of detecting changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee	Yes	Licensee personnel are appropriately trained to assess and conduct an initial

training standards, to assess and conduct an initial response to cyber attack alarm conditions?		response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.13 EXAMPLE 13: MICROPROCESSOR BASED I&C SYSTEM EXAMPLE C

Background

- System utilizes Anti-Virus, HIDS, and Data Loss Prevention Protection.
- System contains several windows-based computers and a number of firmware based components.
- System performs both indication and control functions.
- NIDS is deployed in accordance with defensive strategy at the network boundary.
- Logs are sent to the SIEM for analysis and alerting.
- Vendors without UAA must be escorted while in the plant and while working on the system.
- System does not utilize whitelisting.
- The SIEM deployed in accordance with procedure requirements provides mechanisms to identify and notify individuals of abnormal cyber conditions on the system. Notifications of events identified by the SIEM are forwarded to on call cyber analysts.
- The SIEM collects logs from systems, which support log forwarding.
- Network intuition detection servers monitor communications at the defensive level boundary and notify the on call cyber security analyst of events matching signatures.
- Plant Operators are trained to detect abnormal operation of the equipment and validate inputs using diverse methods.
- This equipment is located in locked cabinets with key control. Some cabinets are alarmed, with a trouble alarm sent to the control room via the PPC to detect unauthorized entry. Most of the equipment is located in the VA.
- Centrally managed Antivirus, Data loss prevention and HIDS software is deployed and monitored by SIEM to detect and prevent malicious software or unauthorized PMD use.
- PMD control provides adequate protection to mitigate and detect the PMD attack vector.
- Procurement of devices in accordance with System and Services Acquisition cyber security controls.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System utilizes Anti-Virus, HIDS, and Data Loss Protection. System contains several windows based computers and a number of firmware based components. NIDS is deployed in accordance with defensive strategy at the network boundary. Logs are sent to the SIEM for analysis and alerting. The licensee implements the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		

Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible because the system is a legacy system and is not supported anymore and the system may become unstable with whitelisting installed. Changes to system software will require design and testing by the vendor or software developer to ensure no unexpected software code is provided with a change.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection indicators are updated as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	The licensee uses anomaly indicators as part of its detection strategy and updates the anomaly indicators as needed. Anomaly indictors are also accomplished as part of the App E section 11 System and Services Acquisition program. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, and installation. Operators monitor plant other confirmatory plant equipment 24/7 and will identify anomalous equipment behavior.
Integrity of the Intrusion Detection System		

If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	The IDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst and CSIRT for monitoring and response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		

Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.14 EXAMPLE 14: TRANSMITTER

This transmitter is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- This remote transmitter is a flow transmitter used to modulate a flow control valve via the Distributed Control System (DCS) associated with an SSEP System. This is located within the PA and VA.
- The attack pathways to this device are by way of Maintenance and Test Equipment (MTE) and the data bus (4-20mA loop) and the supply chain.
- This device is protected by and behind a one-way deterministic boundary device with no bypasses.
- The device functionality is firmware based requiring physical access to change its functionality, however certain configuration parameters are manageable via the data bus.

Where along the attack pathway will the licensee detect a cyber attack?

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable Media__X__

IDS (HIDS/NIDS) _ _

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks	Yes	To address detection, the licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of

before adverse impact to the SSEP function?		malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. Software changes are verified against signature and anomaly based indicators. PMD control program will detect malware on portable devices.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	System does not support whitelisting. CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software. This is equivalent to whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The system does not support IDS or AV and as a result, signature based detection is not technically possible. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software.

		PMD control program will detect use signature based indicators to detect malware on portable media and devices.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indication is not supported by this system. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious, anomalous behavior, and unneeded software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. Operators monitor these systems 24/7 and will be able to detect anomalous behavior of plant equipment.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is not supported on installed equipment, but is supported in equipment used a part of supply chain and acquisition equipment used to ensure adequate testing prior to being installed in plant systems.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with	Yes	Licensee personnel are appropriately trained to assess and conduct an initial

licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?		response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

ADDENDUM 3: SYSTEM AND SERVICES ACQUISITION

1 INTRODUCTION

1.1 BACKGROUND

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

10 CFR 73.54(b)(2) requires licensees to establish, implement, and maintain a cyber security program for the protection of the assets identified in 10 CFR 73.54(b)(1). Further, 10 CFR 73.54(c)(1) requires that the cyber security program must be designed to implement security controls to protect the assets identified in 10 CFR 73.54(b)(1) from cyber attacks.

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 7, provides a template for the implementation of the cyber security plan. NEI 08-09, Appendices D and E provide cyber security controls to assist licensees in meeting the requirements in 10 CFR 73.54(c)(1).

Lessons learned through licensee implementation efforts, and through a series of implementation workshops conducted during 2016 that included industry and NRC observers indicate that clarification regarding acceptable approaches to implement certain cyber security controls is warranted. The clarifications are needed to enhance clarity and consistency in implementation, and to support NRC oversight activities.

The changes in this Addendum are consistent with the cyber security program performance objective to provide high assurance that digital computer and communications systems and networks are adequately protected against the design basis threat of radiological sabotage cyber attack as described in 10 CFR 73.1. The changes in this Addendum are intended to add necessary clarity without decreasing the effectiveness of cyber security plans implemented using the guidance in NEI 08-09.

1.2 PURPOSE

This addendum provides clarification to the cyber security controls documented in NEI 08-09, Revision 7, Appendix E, Section E.11, "System and Services Acquisition."

1.3 SCOPE

The guidance in this addendum is applicable to power reactor licensees with Cyber Security Plans (CSP) based on the template in NEI 08-09, Revision 7. The guidance in this Addendum is applicable to any CDA, and incorporates tailored guidance for licensees that may have used NEI 13-10, "Cyber Security Control Assessments," to assist in implementation of cyber security controls.

1.4 USE OF THIS DOCUMENT

This document may be used to implement the System and Services Acquisition cyber security controls.

1.5 DEFINITIONS

The following terms are used in this document. Definitions for these terms can be found in Appendix B, "Definitions" to NEI 08-09, Revision 7, and are not reproduced here:

- **Commercial Off-The-Shelf (COTS) Software**
- **Custom Software**

2 SYSTEM AND SERVICES ACQUISITION GUIDANCE

This section provides guidance related to the System and Services Acquisition cyber security controls in Appendix E, Section E.11 of NEI 08-09, Revision 7.

2.1 GENERAL GUIDANCE

2.1.1 Applicability

The NEI 08-09, Revision 7, E.11, “Systems and Services Acquisition,” family of cyber security controls apply to the acquisition of CDAs, components of CDAs and services related to CDAs and components of CDAs following a licensees Cyber Security Plan full implementation date. CDAs that have been installed in the plant prior to the Cyber Security Plan full implementation date have already been through the acquisition and the associated licensee installation testing process, thus further action is not necessary to meet the E.11 requirements. The E.11.6 requirement for audits of CDAs are applicable to previously installed CDAs as part of the ongoing monitoring and assessment process. However, E.11 controls are applicable for the ongoing acquisition of parts or services associated with those CDAs.

2.1.2 Maintaining Custody and Control of Devices or Software from a Vendor to Installation

In order to use vendor-testing programs to meet the requirement of NEI 08-09, Appendix E, Section 11.5 requirements as a means to detect malware, the licensee must demonstrate that custody and control of the devices have been maintained from the vendor through the time period that the CDA/CS or software has been installed in the plant.

Licensee receipt processes shall ensure that devices or software were procured and expected to arrive and were received with normal vendor shipping packaging, such as shrink-wrap, tamper seal or other recognizable packaging and marking in place.

Control of the CDA/CS or software package shall be maintained and placed into segregated areas with access controls in place, that at a minimum meet the requirements, if located outside of the PA, of NEI 08-09, Appendix E, Section 5.5, "Physical Access Control," to ensure that only authorized individuals have physical access to the materials while being stored prior to installation. For software, the integrity of the software shall be maintained by verifying integrity of the software before use.

2.1.3 Cyber Security Control Specific Guidance

This section reproduces the cyber security controls from NEI 08-09 and then provides implementation guidance.

2.1.4 Appendix E.11.1, System and Services Acquisition Policy and Procedures

Control language from NEI 08-09

This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, system and services acquisition policy that addresses the following:
  - The purpose of the security program as it relates to protecting the organization's personnel and assets;
  - The scope of the security program as it applies to the organizational staff and third-party contractors;
  - The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments.
- A formal, documented procedure to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Guidance

The objective of System and Services Acquisition Policy and Procedures is to ensure that licensees develop a formal, documented, system and services acquisition policy that addresses cyber security concerns and requirements in their purchase of CDAs and associated services and that licensees develop and deploy policies and procedures that address this objective. Licensees must develop and implement a formal, documented procedure to facilitate the implementation policy and associated system and services acquisition controls.

Applicability of Section E.11 Controls:

- **Safety-Related Direct CDAs** – Licensee Appendix B quality requirements meet many of the requirements of NEI 08-09, Appendix E, Section 11 requirements. Licensees need to ensure that cyber security requirements are included in the Safety-Related design and procurement process and that the gaps between the NEI 08-09,

Appendix E, Section 11 requirements and the safety-related processes are evaluated and closed.

- **Non-Safety Direct CDAs** – The licensee non-safety-related procurement requirements must ensure that cyber security requirements are included in plant procurements programs.

- **Indirect CDAs** – Appendix E, Section 11 controls for Indirect CDAs can be addressed programmatically using normal site procurement standards such as:
  - Approved vendor list,
  - Receipt inspection,
  - Storage of CDAs,
  - Pre-installation testing.

2.1.5 Appendix E.11.2, Supply Chain Protection

Control language from NEI 08-09

This security control protects against supply chain threats by employing the following measures to protect against supply chain threats and to maintain the integrity of the CDAs that are acquired:
- Establishment of trusted distribution paths,
- Validation of vendors, and
- Requirement of tamper proof products or tamper evident seals on acquired products.

Guidance

The objective of this control is to ensure that items (including software) obtained from the supply chain are procured from trusted sources and those critical items have traceability and validation, such as a certification of compliance. The purpose of this control is to ensure that licensees take appropriate measures to protect their supply chain including vendor validation, tamper-proof packaging, and that CDAs meet defined levels of trustworthiness, and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

- Establishment of trusted distribution paths and validation of vendors;

  - Licensees must take reasonable measures to ensure that the vendor is a valid trustworthy business and that the shipping process is secure.
    - Safety-related equipment design and procurement standards may have measures in place to meet these requirements. However, these programs must be validated to meet these requirements or be modified if deficient in order to take credit for these programs.
    - For other Direct CDA procurement, a process must be developed to validate the vendors:

- Validated vendor- Vendors must be evaluated and approved before conducting business. The vendor validation process is intended to ensure that vendors are legitimate commercial entities by confirming their existence. The vendor validation process includes attributes such as:
  - Ensuring a dealer or reseller is authorized by the vendor.
  - Verification of tax information as outlined in the Taxpayer Identification Number Form (W-9).
  - Verification of D-U-N-S number and information.
  - Assessment of influence of Foreign ownership.
  - In addition, vendors may be subject to public domain searches, assessment by a third party service and direct telephone contact from Procurement Services.

- The supplier's process defines the actions taken (e.g. access controls, scanning, testing, etc.) to ensure the integrity of systems and components (including the hardware and software components that compose those systems).
- The licensee must understand the distribution paths and ensure that they comply with program standards.
- For Commercial of the Shelf (COTS)/Catalogue and third-party purchases, the license must ensure that products come from a "validated vendor" which includes shipping from known, designated shipping points and is tested in accordance with section E.11.6.

- Requirements for maintaining custody and control of devices or software, and the use of tamper proof products or tamper proof seals.

  - In order to meet the requirements of NEI 08-09, Appendix E, Section 11.2 requirements, the licensee must demonstrate that the device or software is coming from a known source and that custody and control have been maintained from the vendor through the time period that the CDA/CS or software has been installed in the plant.
  - Licensee receipt inspection processes shall ensure that devices or software are shipped and received with manifest and expected vendor shipping packaging is in place, such as shrink-wrap, tamper seal or other recognizable packaging and marking.
  - Control of the package(s) shall be maintained and placed into segregated areas or are tampered sealed in order to identify attempts at unauthorized access, in locations with access controls in, that at a minimum meet the requirements, if located outside of the PA, of NEI 08-09, Appendix E, Section 5.5 to ensure that only authorized individuals have physical access to the materials while being stored prior to installation.
  - Software should be shipped in tamper evident packaging or protected by encryption, digital signatures and hashing algorithm is used to validate the integrity of software provided by the vendor Software on CDs, DVDs, Flash mass storage or other media that is not protected by tamper-evident packaging should be sent and stored in an encrypted format. Media passwords or access controls should be sent separately from the device.

- In the absence of the above processes, the licensee takes on the responsibility to ensure that the testing in accordance with E.11.6 conducted prior to installation is robust enough to ensure that any known malware and vulnerabilities can be detected and addressed.

2.1.6 Appendix E.11.3, Trustworthiness

Control language from NEI 08-09

This security control requires that CDAs meet defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

Guidance

The objective of the Trustworthiness control is to ensure that acquired or developed software is free from known cyber security vulnerabilities as well as unauthorized and undocumented functionality and features. This security control requires that CDAs meet defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

The referenced requirements document should include applicable Software Quality Assurance (SQA) and cyber security program requirements that detail required actions to manage software quality and minimize the potential for flawed or malformed software.

Safety-related equipment design and procurement standards may have measures in place to meet these requirements but must be verified to ensure they meet these requirements.

For other Direct CS/CDAs and software, detailed purchasing specifications must be developed which includes configuration documentation, configuration validation, factory acceptance testing, and a cyber security program that minimizes flaws.

For catalog purchases, validated vendors under contractual obligations to reduce vulnerabilities must be used. In the absence of these controls, appropriate performance testing in accordance with Section E.11.6 must be completed prior to installation.

2.1.7 Appendix E.11.4, Integration of Security Capabilities

Control language from NEI 08-09

This security control documents and implements a program to ensure that new acquisitions incorporate security controls based on the following:

- Being cognizant of evolving cyber security threats and vulnerabilities;
- Being cognizant of advancements in cyber security protective strategies and security controls; and

- Conducting analyses of the effects advancements could have on the security, safety and operation of the nuclear critical assets, systems, CDAs and networks at their facility.

Guidance

The objective of this control is to ensure that the licensee's cyber security program remains effective over time as the threats, attack methodologies, and corresponding protective and detective measures evolve. The purpose of this control is to ensure that licensees establish guidelines for the integration of security capabilities into organizational acquisitions.

To ensure licensees integrate current security capabilities into new acquisitions:

- Ensure the procurement of CDAs is informed by the vulnerability and threat management program.
- Ongoing Monitoring and Assessment Effectiveness Analysis in accordance with Section 4.4.3.2 of the Licensee CSP considers advancements in protective strategies and security controls that improve performance of the Cyber Security Program and ensures that design and purchasing processes are maintained.
- Design cycle and purchasing process must be maintained to ensure linkage to the defensive strategy and Security Control Implementation Strategy.
- The Supplier or Licensee should document a cyber security impact analysis or other analysis that considers how assets could be exploited and the potential impacts of security control failures on CDA security and safety functions.
- New acquisitions incorporate program effectiveness and address potential vulnerabilities as they evolve in response to changing threats.
- The Licensee should work with the Supplier and have a process that ensures CDAs are developed and delivered in a way that addresses known vulnerabilities and considers potential failure modes. The engineering change process typically will ensure that these failure modes would be evaluated for impacts on functionality.
- For COTS/catalogue purchases, if there is no or limited support by vendor programs or processes, the licensee is responsible for the role of the integrator and needs to address evolving cyber security threats and vulnerabilities and CDA failure modes and effects on SSEP functions and appropriate testing in accordance with Section E.11.6 prior to installation.

2.1.8 Appendix E.11.5, Developer Security Testing

Control language from NEI 08-09

This security control requires system developers/integrators of acquired CDAs create a security test and evaluation plan, implement the plan, and document the results such that:

- The products are delivered to meet specified security requirements, and
- The delivered product is free from known testable vulnerabilities and known malicious code.

This security control also requires the plan and results be reviewed and approved by the licensee.

Guidance

The objective of developer security testing is to ensure that purchased software, or software delivered as a component of a CDA, is free of malicious, hidden, and/or unauthorized content or functionality and known vulnerabilities.

When the licensees utilize a third-party vendor to develop and acquire a CS/CDA, licensees should specify requirements for factory acceptance functional testing as part of the purchasing contract and ensure that the contract is augmented to include testing of the cyber security control implementations. As part of the control, licensees must review and approve security testing.

A Cyber Security procurement specification addresses:

1. Requirements for a CDA security evaluation and testing plans to demonstrate proper security control capabilities and functionality.
2. A Licensee requirement to review and approve CDA security evaluation and testing plans.
3. CDA security evaluation and testing plans that include actions that provide reasonable assurance the delivered product is free from known testable vulnerabilities and known malicious code.
4. A Supplier process that includes steps that maintains the integrity of developed CDA software until the product is delivered.

For devices where there is no or limited knowledge of vendor programs or processes, such as for COTS/catalogue purchases, appropriate CDA Performance Testing must be performed prior to installation.

2.1.9 Appendix E.11.6, Licensee Testing

Control language from NEI 08-09

This security control:

- Requires testing (e.g., off-line on a comparable CDA) of security devices and software to ensure that they do not compromise the CDA or interconnected CDAs operation prior to installation, and
- Deploys security controls and flaw remediation measures based on reliable and credible sources of risk information.

This security control requires audits of CDAs, to provide high level of assurance that the safety, security, and emergency preparedness function are protected from a cyber-attack to validate the following items:

- Security controls present during system validation testing are still installed and operating in the production system,
- CDAs are free from known security compromises and continue to provide information on the nature and extent of compromises should they occur, and
- Management of change program is being followed with an audit trail of reviews and approvals for changes.

Guidance

The objective of this control is to ensure that CDAs are tested for vulnerabilities and effective security controls prior to introduction into a production environment or network, as well as throughout the system's lifecycle.

Licensees' programs should ensure that site acceptance testing is specified in the design cycle and procurement contract, and that site acceptance testing includes validation of the cyber security control implementation. Configuration management activities must provide an audit trail of subsequent changes.

The programs include:

1. Site acceptance testing that validates proper security control capabilities and functionality prior to placing the CDA into production.
2. A documented vulnerability assessment or scan that concludes the installed CDA configuration is free from known vulnerabilities and known malicious code.
3. Requirements that changes made during installation and final testing are controlled in accordance with licensee configuration change control processes.

For devices where developer or vendor programs cannot be verified, such as for COTS/catalogue purchases and untrusted sources the license must ensure that appropriate controls are in place and testing as described below is conducted to ensure that CDA/CS and software have no vulnerabilities or malware prior to installation.

For complex or purpose built CDAs/CSs or software, where feasible, testing shall include:

- Testing of a CS/CDA in an isolated test environment, where the CS/CDA is then functionally tested to meet a formal documented hardware and/or software requirements testing plan and the software quality assurance plan.
- Third party software products, which have been integrated into a software derivable product, shall be disclosed and known vulnerabilities identified. Software testing shall include input parameter testing of both valid and invalid input conditions to verify those conditions will not adversely affect the system/device. Software shall be tested against known testable vulnerabilities that would allow an attack to compromise the systems/device.

For COTS catalogue purchases, and untrusted vendor sources where the above testing cannot be accomplished; vendor testing cannot be determined, or adequate custody and control of the Digital Asset from the vendor to the licensee site until installation in the plant is not maintained:

- Perform a thorough visual inspection looking for obvious signs of tampering, chip replacement, circuit modifications, non-OEM replacement parts, missing or obfuscated part identifiers, etc.;
- If possible, determine what software development and QA is performed by the vendor, in order to take credit for the signature and performance testing that will reveal anomalous behavior;
- If unable to determine the testing performed by the vendor, perform functional testing as described below:

    - For low functioning, non-field modifiable devices (NEI 13-10, Appendix D, A.1, A.2 devices):
        - Signature base scans, if feasible; and,
        - Functional testing.

    - For more complex devices (NEI 13-10, A.3 and higher):
        - Flash or wipe the device and re-image with controlled software and conduct functional testing; and,
        - Conduct vulnerability and malware scans of the device.

    - For complex devices that cannot be flashed or wiped clean:
        - Vulnerability and malware scan of the device; and,
        - Conduct expanded functional testing to consist of input testing for both valid and invalid input conditions to verify that those conditions will not adversely affect the system/device.

ADDENDUM 4: PHYSICAL ENVIRONMENT PROTECTION

1 INTRODUCTION

1.1 BACKGROUND

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

10 CFR 73.54(b)(2) requires licensees to establish, implement, and maintain a cyber security program for the protection of the assets identified in 10 CFR 73.54(b)(1). Further, 10 CFR 73.54(c)(1) requires that the cyber security program must be designed to implement security controls to protect the assets identified in 10 CFR 73.54(b)(1) from cyber attacks.

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 7 dated April 2010, provides a template for the implementation of the cyber security plan. NEI 08-09, Appendices D and E provide cyber security controls to assist licensees in meeting the requirements in 10 CFR 73.54(c)(1).

Lessons learned through licensee implementation efforts, and through a series of implementation workshops conducted during 2016 that included industry and NRC observers indicate that clarification regarding acceptable approaches to implement certain cyber security controls is warranted. The clarifications are needed to enhance clarity and consistency in implementation, and to support NRC oversight activities.

The changes in this Addendum are consistent with the cyber security program performance objective to provide high assurance that digital computer and communications systems and networks are adequately protected against the design basis threat of radiological sabotage cyber attack as described in 10 CFR 73.1. The changes in this Addendum are intended to add necessary clarity without decreasing the effectiveness of cyber security plans implemented using the guidance in NEI 08-09.

1.2 PURPOSE

This addendum provides clarification to the cyber security controls documented in NEI 08-09, Revision 7, Appendix E, Section E.5, "Physical Environment Protection."

1.3 SCOPE

The guidance in this addendum is applicable to power reactor licensees with Cyber Security Plans (CSP) based on the template in NEI 08-09, Revision 7. The guidance in this Addendum is applicable to any CDA and incorporates tailored guidance for licensees that may have used NEI 13-10, "Cyber Security Control Assessments," to assist in implementation of cyber security controls.

1.4 USE OF THIS DOCUMENT

This document may be used to implement the Physical Environment cyber security controls.

1.5 ACRONYMS

The following acronyms are used in this document:

E.5 – Cyber security controls in Section 5 of Appendix E to NEI 08-09
PA – Protected Area
VA – Vital Area

2 PHYSICAL ENVIRONMENT PROTECTION GUIDANCE

This section provides guidance related to the Physical Environment Protection cyber security controls in Appendix E, Section E.5 of NEI 08-09, Revision 7.

2.1 GENERAL GUIDANCE

The NEI 08-09, Revision 7, Appendix E, Section E.5, "Physical Environment Protection," cyber security controls addressed in this guidance apply to Critical Digital Assets (CDAs), including those assessed under NEI 13-10 as both Direct and non-Direct and that are located outside of the Protected Area (PA) of nuclear power plant. As described in NEI 13-10 Section 5, "Baseline Cyber Security Protection Criteria," the E.5 controls are not required for Emergency Preparedness CDAs that have been assessed as having their function maintained by alternative means. However, if an EP CDA provides a pathway to a CDA(s) that would have an adverse impact to a safety or security function, this guidance shall apply.

The physical security controls in NEI 08-09, Appendix E, Section E.5, provide physical access control to delay and detect and respond to unauthorized physical access to CDAs which are located outside the PA. However, the E.5 controls are not meant to be equivalent to those required under 10 CFR 73.55 for physical protection of the PAs and Vital Areas (VAs) of a nuclear power plant. As a result, licensee corporate security or third-party solutions may be used for addressing the E.5 controls.

For Direct and non-Direct CDAs outside the PA, the E.5 physical security controls are very important in addressing the technical security controls provided in licensee cyber security plans. Specifically, the physical security controls and physical isolation of non-Direct CDAs eliminate many of technical controls provided in the cyber security plan. Therefore, the intent of each of the security controls provided in E.5 needs to be met for CDAs to be maintained as non-Direct.

2.2 CYBER SECURITY CONTROL SPECIFIC GUIDANCE

The E.5 family of cyber security controls implements and documents physical protections for CDAs located outside the PA. Physical protections for CDAs located inside a PA or VA are provided by the Physical Security Plan to comply with 10 CFR 73.55.

This section reproduces the cyber security controls from NEI 08-09 and then provides implementation guidance.

2.2.1 Appendix E.5.1, Physical Environment Protection Policies and Procedures

Control language from NEI 08-09

For those CDAs located outside of the protected area, develop, implement, review in accordance with 10 CFR 73.55(m), and update:

- A formal, documented physical environment protection policy that addresses:
  - The purpose of the physical security program as it relates to protecting the CDAs;
  - The scope of the physical security program as it applies to the organization's staff and third-party contractors;
  - The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with security policies and other regulatory commitments.
- Formal, documented procedures to facilitate the implementation of the physical environment protection policy and associated physical environmental protection security controls.

Guidance

This control applies to CDAs that are located outside the PA and VA.

2.2.2 Appendix E.5.2, Third Party/Escorted Access

Control language from NEI 08-09

This security control consists of:

- Screening, enforcing and documenting security controls for third-party personnel and monitoring service provider behavior and compliance. Third-party providers include service contractors and other organizations providing control system operation and maintenance, development, IT services, outsourced applications, and network and security management.
- Including personnel security controls in acquisition-related contract and agreement documents.

Guidance

One way to address the controls provided in E.5.2 is by using existing site physical security processes for PA or other processes that implement controls that meet the same security criteria for controlling the access of third parties or other personnel not cleared for unescorted access and screening and appropriately escorting when gaining access to locations with CDAs.

2.2.3 Appendix E.5.3, Physical & Environmental Protection

Control language from NEI 08-09

This security control consists of securing and documenting physical access to CDAs. Physical security controls (e.g., physically isolated environment, locked doors, etc.) are employed to limit access to CDAs.

Guidance

One way to address the controls provided in E.5.3 is by ensuring that CDAs are located in areas/facilities with robust walls, ceilings, and doors to prevent unauthorized access or entry. Locks, access control entry devices (i.e., key cards), or other means to ensure isolation and protection of CDAs should be implemented in a way that ensures positive control and appropriately facilitates assessment of unauthorized access. This control works in conjunction with the other E.5 controls to ensure protection, assessment and response to intrusions and should include the use of technologies such as tamper indicating devices and/or cameras or other means to assess the extent of an unauthorized entry into an area outside the PA with CDAs

2.2.4 Appendix E.5.4, Physical Access Authorizations

Control language from NEI 08-09

This security control consists of:

- Developing and maintaining a list of, and issuing authorization credentials (e.g., badges, identification cards, smart cards) to, personnel with authorized access to facilities containing CDAs and security boundary systems.
- Designating officials within the organization to review and approve the above access lists and authorization credentials, consistent with the access authorization program.

Guidance

One way to address the controls provided in E.5.4 is by using the existing site physical security processes for the PA or other processes that ensure personnel are screened and only authorized personnel are issued credentials that will allow access to the areas with CDAs outside the PA. A designating official shall be identified and shall perform reviews and approval of access decisions and ensures that periodic reviews of authorized individuals be often enough to ensure that the list remains current to protect the SSEP functions or Direct CDAs described in NEI 13-10 from cyber compromise of the CDAs by unauthorized individuals.

2.2.5 Appendix E.5.5, Physical Access Control

Control language from NEI 08-09

This security control consists of:

- Controlling physical access points (including designated entry/exit points) to locations where CDAs reside and verify individual access authorization before granting access to these areas.
- Approving individual access privileges and enforces physical and logical access restrictions associated with changes to CDAs.
- Controlling logical access through the use of electronic devices and software.
- Generating, retaining, and reviewing records pertaining to access restrictions.
- Ensuring qualified and authorized individuals obtain access to CDAs.
- Controlling physical access to CDAs independent of the physical access controls for the facility.

Guidance

This control requires that access to CDAs are controlled through designated entry and exit locations and that measures are in place to verify current access authorization has been only granted in accordance with E.5.4 above. Third parties or individuals not authorized unescorted access must be processed and escorted in accordance with E.5.2.

Control of designated entry and exit points can be accomplished through the use of both manual and electronic methods. If employing manual means, such as door locks or padlocks, existing physical security key control program or other similar program must be in place to ensure only authorized personnel have access to keys, and measures must be in place to re-key locks upon loss of control of keys or changes of personnel with access to controlled keys.

If electronic devices and software, such as card readers, are used to control entry, measures must be in place to detect attempts to tamper or bypass these systems. Logical access to these systems and software must be controlled and measures must be in place to ensure that only qualified individuals with authorized unescorted access can gain access to CDAs.

If CDA(s) are located in a facility that has access controls for a larger population of individuals that do not require or are not qualified for access to the CDAs, there must be additional barriers and access control to restrict access to CDA(s) to only those qualified, requiring access, and authorized in accordance with Section 5.4 above.

CDAs in facilities or locations outside the control of the licensee, such as a switchyard owned by another company or part of the non-nuclear distribution division of a company, must be protected in accordance with this control.

However, for the BOP CDAs described in NEI 13-10, the physical access controls that are in place to meet North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards are sufficient to meet this requirement as long as:

- Formal agreements are in place to maintain these controls and only allow access to CDAs by personnel authorized by the licensee; and,

- The licensee security and other organizations are timely notified of potential tampering or attempted bypass, and any attempt to compromise a CDA through unauthorized access is detected and mitigated before adverse impact to safety or security function or Direct CDAs described in NEI 13-10.

For other locations outside the licensee's control, with no physical access control requirements, the licensee must ensure that adequate access control measures are in place for these CDAs to meet the objectives of the security controls provided in E.5.5. Physical locks or electronic means on the CDAs that are under the control of the licensee may be used to address these security controls by meeting the objectives of the security controls provided in E.5.5.

2.2.6 Appendix E.5.6, Access Control for Transmission Medium

Control language from NEI 08-09

This security control consists of controlling and documenting physical access to CDA communication paths.

Guidance

CDA transmission communications paths must be adequately controlled outside the PA to ensure that no unauthorized access or tampering has occurred. Underground cables must be placed in metallic or other similarly strong conduit material buried underground or imbedded in one foot of concrete to prevent the cable being dug up without being observed by OCA patrols, cameras or other means.

Access to cable that transitions a short distance from underground outside to the inside of secure buildings must be controlled by being run in metallic or other similarly strong conduit material, must not have un-monitored access panels, be hung aerially on poles, or be in open cable trays or under floors. Cabling conduit in this transition area must be subject to periodic and random observation at frequencies similar to that performed by the site OCA patrols or cameras.

Tamper indicating technology, assessment and response may also be used on transmission media systems to supplement protection if unable to satisfy some of the elements above.

2.2.7 Appendix E.5.7, Access Control for Display Medium

Control language from NEI 08-09

This security control consists of controlling and documenting physical access to CDAs that display information that may assist an adversary to prevent unauthorized individuals from observing the display output.

Guidance

Access to CDAs that display security sensitive information must be controlled in accordance with licensee processes and procedures for handling CDAs located inside the PAs to prevent the unintended and unauthorized disclosure of sensitive information through its visual presentation on a CDA-driven display. The scope of the sensitive information covered includes but is not limited to security sensitive and SGI information, passwords or codes entered on a keypad, and other information that can assist in compromising the CDAs.

2.2.8 Appendix E.5.8, Monitoring Physical Access

Control language from NEI 08-09
This security control consists of:

- Monitoring and documenting physical access to CDAs and security boundaries to detect and respond to physical security incidents. For incidents, reviews physical access logs and coordinates results of reviews and investigations with the incident response personnel.
- Monitoring real-time physical intrusion alarms and surveillance equipment.
- Employing automated mechanisms to assess and recognize potential intrusions and initiates appropriate response actions.
- Providing lighting for access monitoring devices (e.g., cameras).

Guidance

Monitoring physical access, documenting and reviewing logs and alarms must be accomplished in accordance with existing or similar plant processes for the PA to meet the intent of the security controls provided in Section 2.2.7 (Appendix E.5.8, Access Control for Display Medium). A corporate level or third-party monitoring capability may be used, but the licensee must also ensure that agreements are in place to:

- Monitor and document physical access to CDAs and security boundaries to detect and respond to physical security incidents. For incidents, reviews physical access logs and coordinates results of reviews and investigations with the incident response personnel.

- Monitor real-time physical intrusion alarms and surveillance equipment.

- Employ automated mechanisms to assess and recognize potential intrusions and initiate appropriate response actions.

- Provide lighting for access monitoring devices (e.g., cameras).

Use of surveillance equipment (e.g., cameras) with appropriate lighting, alarm monitoring, and response times must be commensurate with the CDA pathways and access to plant Safety and Security systems. For equipment that provides a pathway to systems or assets performing or supporting a safety or security function, real time monitoring and surveillance equipment is implemented to ensure assessment and prompt response to intrusions are commensurate with physical security response times to alarms associated with safety and security equipment inside the PA.

The following can be used for CDAs that are: considered isolated; are located in licensee access controlled facilities; do not have any pathways to other systems; are of limited functionality; and, whose compromise will have limited and easily quantifiable consequences (e.g. X-Ray Machine):

- Use of identifiable tamper indicating devices that provide verification that no unauthorized access to the digital device has occurred;

- Performing periodic surveillance of tamper indicating devices; and

- Perform periodic functional and operational checks sufficiently often to ensure that the cyber compromise of the CDA can be detected in time to mitigate the compromise before adverse impact to safety or security functions or Direct CDAs described in NEI 13-10.

For Balance-of-Plant (BOP) CDAs, described in NEI 13-10, whose failure or cyber compromise could cause a reactor scram/trip, and that are located in facilities that are outside the PA or locations outside the control of the licensee, such as a switchyard owned by another company or part of the non-nuclear distribution division must have real time physical monitoring and surveillance in place by a corporate or third party provider and formal agreements to maintain these controls, restrict access to CDAs by unauthorized personnel, and allow timely licensee response to indications of tampering or bypass of the access controls to comply with NERC CIP Reliability Standards associated with monitoring physical access to these CDAs.

2.2.9 Appendix E.5.9, Visitor Control Access Records

Control language from NEI 08-09

This security control consists of:

- Controlling and documenting visitor physical access to CDAs by verifying the identity and confirming access authorization of these individuals prior to entry.
- Escorting visitors and monitoring visitor activity to prevent adverse impact to safety, security and emergency preparedness functions.

Guidance

Visitor control access records must be controlled in accordance with existing processes and procedures for the CDAs located inside the PAs or similar licensee processes and procedures.

ADDENDUM 5: CYBER SECURITY VULNERABILITY AND RISK MANAGEMENT

1 INTRODUCTION

1.1 BACKGROUND

Nuclear licensees are required in accordance with Appendix A Sections 4.4.2, 4.4.3.2 and 4.9.1 of their Cyber Security Plans (CSP) to address ongoing threats and vulnerabilities to critical digital assets (CDAs) by performing vulnerability assessments or scans and evaluations to identify applicable corrective actions required to mitigate/remediate vulnerabilities to maintain adequate defense-in-depth and prevent CDA compromise or exploitation. The NEI 08-09 Appendix D5.5 (Installing Operating Systems, Applications, And Third-Party Software Updates), and Appendix E3.2 (Flaw Remediation), E3.5 (Security Alerts and Advisories), E9.8 (Contacts with Security Groups and Associations) and E12 (Evaluate and Manage Cyber Risk) provide additional guidance on how to address CSP requirements related to vulnerability and threat management.

1.2 PURPOSE

This addendum documents the process and considerations associated with performing CDA vulnerability assessments. This addendum intends to enhance clarity and consistency in Licensee implementation of vulnerability assessment activities and support NRC oversight activities.

1.3 SCOPE

The guidance in this addendum is applicable to power reactor licensees with CSPs based on the template in NEI 08-09, Revision 7. The guidance in this Addendum is applicable to vulnerability assessment activities associated with CDAs and devices such as security boundary devices and PMMD scanning/transfer systems that protect CDAs from potential compromise or exploitation.

Section 2 describes inventory and screening activities associated with identifying applicable CDA specific vulnerabilities that require further Licensee evaluation and assessment. Section 3 describes the Licensee assessment process for applicable, risk-significant CDA vulnerabilities and includes an example. The example is intended to illustrate considerations and the level of recommended detail for conducting vulnerability assessments.

1.4 USE OF THIS DOCUMENT

This document is intended to be a guide that details an acceptable approach for performing CDA vulnerability assessment activities that address ongoing threats and vulnerabilities to CDAs consistent with the requirements of Sections 4.4.2, 4.4.3.2 and 4.9.1 of Licensee CSPs.

1.5 ACRONYMS

The following acronyms are used in this document:

ALNOTS – ALert and NOTification System CAP – Corrective Action Program

CDA – Critical Digital Asset

CVE – Common Vulnerabilities and Exposures CVSS – Common Vulnerability Scoring System

CSP – Cyber Security Plan

ICS-CERT– Industrial Control System Cyber Emergency Response Team INPO – Institute of Nuclear Power Operations

NVD – National Vulnerability Database PMMD – Portable Media and Mobile Devices SGI – Safeguards information

SSEP – Safety-related and important-to safety functions, Security functions, and Emergency Preparedness functions including offsite communications

US-CERT – United States Computer Emergency Readiness Team

1.6 DEFINITIONS

The following terms are used in this document. Definitions for these terms can be found in Appendix B, "Definitions" to NEI 08-09, Revision 7, and are not reproduced here:

- **ALNOTS**
- **Mitigation**
- **Remediation**

2 VULNERABILITY IDENTIFICATION, SCORING AND SCREENING

2.1 VULNERABILITY IDENTIFICATION

To support CDA security control assessment activities associated with full CSP implementation, Licensees grouped CDAs based on vendor manufacturer, model number and other considerations.
As part of on-going monitoring and assessment and in order to support the vulnerability management process, Licensees need to develop and maintain an inventory of their grouped CDAs based upon different manufacturer and model numbers for their CDA inventory.

Applicable CDA specific vulnerabilities can be identified by comparing Licensee grouped CDA manufacturer and model number information against publicly available vulnerability information documented on the US-CERT, ICS-CERT and National Vulnerability Database (NVD) web site resources. Because there are thousands of vulnerabilities documented in the NVD web site, the use of an automated software tool such as the Institute of Nuclear Power Operations (INPO) hosted Cyber Security ALert and NOTification System (ALNOTS) to identify applicable CDA specific vulnerabilities is recommended to minimize the potential for human error and failure to identify applicable CDA vulnerabilities.

Licensees have addressed the CSP and security controls guidance above by developing a threat

and vulnerability management process. This process includes the use of automated tools such as the INPO hosted ALNOTS or manual searches of CDA specific vulnerabilities documented on the US-CERT, ICS-CERT and NVD web sites against Licensee grouped CDA data to identify applicable CDA vulnerabilities that require further Licensee consideration.

2.2 VULNERABILITY SEVERITY SCORING

Device specific vulnerabilities can be noticed on the US-CERT, ICS-CERT and NVD. Device specific vulnerabilities from the US-CERT, ICS-CERT and NVD that are assigned a Common Vulnerabilities and Exposures (CVE) number are available from NVD. Each vulnerability with an assigned CVE number is also assigned a Common Vulnerability Screening System (CVSS) severity score. The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS severity scores are risk-based calculations that includes consideration of several vulnerability variables such as exploitability, attack vectors, complexity and impact. The NVD currently utilizes two (2) methodologies referred to as the CVSS v2.0 and v3.0 severity scores. The NVD CVSS v2.0 and v3.0 quantitative and qualitative severity scoring systems are shown in Table 2-1 below.

Table 2-2 – CVSS v2.0 and 3.0 Severity Scores

CVSS v2.0 Ratings		**CVSS v3.0 Ratings**	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Because the CVSS v2.0 and v3.0 Base and Environmental scoring schemas differ, it is common for the NVD to notice a v2.0 and v3.0 score with different numerical values. It is less common for the v2.0 and v3.0 severity ratings (Low, Medium or High) to differ. Most of the CVSS v2.0 and v3.0 severity ratings (Low, Medium or High) are the same. It is also common for the CVSS scores to change when new information about a vulnerability and its exploitability becomes available. CVSS scores assess the relative severity of a vulnerability when compared to other vulnerabilities and do not take into account any security controls that might mitigate exploitation attempts (e.g., firewalls, antivirus software, intrusion detection and prevention systems, authentication mechanisms, etc.). CVSS scores are intended as an aid in assessing the potential risk and severity of vulnerabilities and to assist with decision making.

2.3 VULNERABILITY SCREENING

Applicable device specific vulnerabilities, also commonly referred to as CVEs, which require further consideration should be screened using the CVSS v3.0 score when available. When a CVSS v3.0 score is not available, the CVSS v2.0 score should be used in the screening process. The CVSS v3.0 score is preferred because it represents the most current methodology for calculating vulnerability risk and severity. Because the CVSS v2.0 and v3.0 severity scores can differ, it is possible for one severity score to be greater than 7.0 while the other is below 7.0. The number of vulnerabilities that would screen out because the CVSS v3.0 score was less than 7.0 while the v2.0 score was greater than 7.0 is anticipated to be a low. If the licensee consistently uses the CVSS v3.0 or v2.0 score for all vulnerability assessments, then no additional action is needed when the scores are different. If the licensee does not consistently use a single CVSS score, then the licensee should use the higher score when the scores differ.

As mentioned previously, it is common for CVSS scores to change when new information about a vulnerability and its exploitability becomes available. Licensees using ALNOTS or similar automated software tools should screen for modified CVE notices as part of the process that addresses CSP requirements to check for new vulnerabilities in accordance with the NEI 08-09, E12 “Evaluate and Manage Cyber Risk” security control. If a Licensee performs initial screening for a new CVE and the CVSS score was less than 7.0 and that CVE is later modified by the NVD and re-noticed with a CVSS score above 7.0, the potential exists for a Licensee to fail to further evaluate that CVE. Licensees should monitor for changes in CVE CVSS scores that necessitate screening in vulnerabilities that may have previously screened out.

If Licensees choose to perform a vulnerability assessment in lieu of scanning, they must complete a documented vulnerability assessment for applicable device specific vulnerabilities with a CVSS score of 7.0 or higher. The justification for using CVSS scores greater than or equal to 7.0 as a screening criterion for vulnerabilities include the following reasons:

- Milestone 3 Network Defensive Architecture Requirements – Licensee Milestone 3 CSP requirements included defensive architecture changes that restricted or prohibited bi-directional communications with CDAs in the two (2) innermost security levels. CVSS scoring includes consideration for local, adjacent, and remote network access.

- Actual calculated CVSS severity ratings for nuclear Licensees would typically be lower because CDAs in the two (2) innermost security levels are either deterministically-isolated via a data diode or air-gap isolated.
- Defense-in-Depth – CVSS scores assess the relative severity of a vulnerability when compared to other vulnerabilities and do not take into account security controls that might mitigate exploitation attempts (e.g., firewalls, antivirus software, intrusion detection and prevention systems, authentication mechanisms, etc.). Licensees are required to have and maintain several security controls that establish a robust defense-in-depth security posture.
- Cyber Risk and Severity – the CVSS scoring criteria is widely used to qualify and assign risk to vulnerabilities and allows for prioritization based on potential exploitability and consequence. Vulnerabilities with a severity rating of "High" or "Critical" that pose the greatest risk to SSEP functions are screened in and further evaluated to identify the vulnerability attack vectors and Licensee security controls in place that protect the CDA from exploitation. Vulnerabilities with a CVSS severity score of less than 7.0 are qualified as "Low" and "Medium" risk and are less likely to be exploited and/or the impacts of exploiting the vulnerability are not expected to be as significant, therefore "Low" and "Medium" risks are not anticipated to weaken defense-in-depth protections to the point where remediation or mitigation corrective actions to prevent potential exploitation are needed.

Excluding the special considerations cited below for digital devices with a potential high impact and consequence if compromised, applicable device vulnerabilities with a CVSS score of less than 7.0 (Low and Medium severity ratings) can be screened out and do not require a documented evaluation, remediation or further corrective actions.

Special considerations should be given when performing vulnerability screening for those digital assets that, if compromised, could potentially have a high adverse impact or consequence. This population includes digital devices such as one-way deterministic (e.g., Data Diodes) and firewall security boundary devices, portable media scanning stations and centralized monitoring devices (e.g., SIEM and IDS). To support the justification of using a CVSS score of 7.0 or higher for screening CDAs within a protected boundary, licensees must use a CVSS cut-off score of 4.0 (Medium) instead of 7.0 (High) for screening vulnerabilities for these assets.

3 VULNERABILITY ASSESSMENTS

Vulnerability assessments consist of performing a documented evaluation of an applicable CDA specific vulnerability to identify the security controls in place that currently protect against the attack vectors associated with the vulnerability. Vulnerability assessments also identify if existing security control protections are effective in protecting CDA SSEP functions and when those protections could be weakened by the vulnerability to the point that remediation or mitigation corrective actions are required to maintain adequate defense-in-depth.

3.1 VULNERABILITY ASSESSMENT CONSIDERATIONS

Attachment 3-1 provides a vulnerability assessment template that can be used to aid in a consistent approach for performing applicable CDA specific vulnerability assessments.

Vulnerability assessments should consider the following:

- NVD CVE information identifies the attack vectors associated with each vulnerability. The attack vectors associated with each vulnerability and how an adversary might exploit the vulnerability should be documented in the assessment.
- Existing security controls provide protections that may address the applicable attack vectors and exploit associated with a vulnerability. Existing security controls that protect a CDA from potential exploit should be documented in the assessment.
- When existing security control protections are identified as being less than adequate or potentially ineffective in protecting the CDA's SSEP function or when those protections are weakened by the vulnerability to the point that adequate defense-in-depth no longer exists to protect the CDA's SSEP functions, corrective actions to remediate or mitigate the threat should be identified as part of the assessment process.
- Vulnerability assessments and corrective actions for Security system devices may be classified as safeguards information (SGI). Consult and discuss Security system device vulnerability assessment results with Security management prior to documenting them in the site Corrective Action Program or other shared repositories.

Vulnerability assessment documentation retention should comply with Section 4.13 Document Control and Records Retention and Handling of the CSP.

3.2 VULNERABILITY ASSESSMENT ACTION TRACKING

Because corrective actions to address applicable vulnerabilities will often require plant design or configuration changes, planned corrective actions associated with CDA remediation and mitigation should be identified and tracked in the site Corrective Action Program (CAP). Vulnerabilities that significantly erode existing security controls and defense-in-depth may require short-term mitigation actions until long-term remediation actions can be planned and implemented in accordance with applicable Licensee configuration control processes.

Table 3-2 - CDA Vulnerability Assessment Template

CDA Vulnerability Assessment	
CDA Grouping:	
Vulnerability Description:	
Vulnerability Ref Number(s):	
Vulnerability Release Date:	
CVSS Score (v3.0 preferred)	
What attack vectors (Physical access, supply chain, portable media or mobile device, wired connectivity or wireless connectivity) would be applicable in attempting to exploit the vulnerability?	
Identify the security controls are currently in place that protect the CDA from exploitation of the vulnerability as described in the alert or notification document?	
Describe how the existing security controls prevent the vulnerability from being exploited.	
Document recommended short and/or long-term corrective actions to mitigate or remediate the vulnerability when the assessment concludes corrective actions are needed to maintain adequate defense-in-depth.	
Condition Report Number (when required to track corrective actions)	
Cyber Security Program Manager or his designee approval (Print/Sign)	
Date	

4 REMEDIATION OF VULNERABILITIES IDENTIFIED IN CDAS

As stated in Section 1 of this addendum, Appendix A Sections 4.4.2, 4.4.3.2, and 4.9.1 of the licensee Cyber Security Plans (CSP) requires licensees to address ongoing threats and vulnerabilities to critical digital assets. This commitment is met by performing vulnerability assessments or scans, and evaluations to identify applicable corrective actions to mitigate/remediate vulnerabilities while maintaining adequate defense-in-depth and preventing a CDA from becoming compromised or exploited. This supplemental guidance addresses acceptable methods to remediate those vulnerabilities. Methods of evaluation and remediation are the primary purpose of this guidance.

5 EVALUATION OF ATTACK VECTORS

An *attack vector* reflects the context by which vulnerability exploitation is possible. An attack vector is not a vulnerability, exploit, or malware. Publicly disclosed vulnerabilities are assigned one of four values for attack vector: network, adjacent network, local, and physical. A description of each attack vector metric value can be found in the latest Common Vulnerability Scoring System Specification Document.

Vulnerabilities can be exploited, but not attack vectors, or pathways. Attack vector and attack pathway are sometimes used synonymously; however, attack vector is the preferred term because it is the one used by CVSS (Common Vulnerability Scoring System).

A *vulnerability* is a flaw in the design, implementation, or configuration of software that has security implications. Vulnerabilities are classified by their severity (i.e., CVSS base score). CVSS scores are mapped to qualitative ratings of *Critical, High, Medium, Low*, and *None*. To distinguish between different vulnerabilities, they are assigned CVE (Common Vulnerability and Exposure) IDs and might be given a name. For example, *BlueKeep* refers to a specific vulnerability (CVE-2019-0708) in Microsoft's Remote Desktop Protocol (RDP) implementation. This vulnerability is assigned the attack vector metric value of "*Network*" because the vulnerable component is bound to the network stack (RDP listens on port number 3389, by default) and it can be exploited *at the protocol level* one or more network hops away (e.g., across one or more routers). The vulnerability's attack vector is "*Network*", not RDP port 3389.

An *exploit* is a piece of code or a program that takes advantage of a weakness in software or system. Exploits are typically classified by the resulting behavior after a vulnerability is exploited, such as arbitrary code execution, privilege escalation, denial of service, or data exposure. Exploits might sometimes be given a name. For example, *EternalBlue* refers to code written to exploit multiple vulnerabilities in Microsoft's Server Message Block version 1 (SMBv1) protocol. The most severe of the vulnerabilities (i.e., those with a higher CVSS score) could allow *remote code execution* if an attacker sends specially crafted messages to a vulnerable (unpatched) SMBv1 server over a network. The attack vector of the SMBv1 vulnerabilities *exploitable by EternalBlue* is "*Network*". The exploit is not an attack vector. Attackers or malware, leverage exploits to achieve their end goal.

Malware is classified by the payload or malicious action it performs. Malware must be delivered, for example, across a network or via physical media, to a target system and then executed. For example, *WannaCry* is a specific type of malware (ransomware) that uses the *EternalBlue* exploit to spread itself across a network infecting all connected devices and dropping a crypto-ransomware payload. The attack vector of the *exploited* vulnerability is "*Network*" even if the malware is initially transferred to a system using portable media.

CVSS metrics do not account for threats presented by the supply chain or use of portable media and devices. With respect to these vectors, the concern is with introducing, or delivering, "patches, software updates, replacement firmware, replacement hardware/components that contain malicious and/or detrimental elements such as time-bomb logic, unauthorized backdoors, hidden functionality, degraded components, faulty designs, etc., that can adversely impact the functionality of the CDA". The supply chain, portable media, and devices are an indirect means to introduce malware into a target system; they are not attack vectors from the perspective of vulnerabilities.

Appendix E, Section 3.5 requires licensees to "receive security alerts, bulletins, advisories, and directives from credible licensee-designated external organizations on an ongoing basis". Examples of a credible external organization are the U.S. government's Cybersecurity & Infrastructure Security Agency (CISA) and NERC's Electricity Information Sharing and Analysis (E-ISAC).

Security alerts and advisories provide information related to observed threat activity and publicly disclosed vulnerabilities to raise situational awareness regarding new threats, campaigns, and incidents and to notify users about security issues affecting vendor products.

When reviewing alerts and advisories pertaining to specific threats (e.g., malware) or threat activity, licensees should ensure associated vulnerabilities are assessed and addressed.

Consider *SUNBURST backdoor/*SolarWinds supply chain attack. *SUNBURST* is malware, not a vulnerability (*SUNBURST* doesn't have any assigned CVE IDs). A licensee could have unwittingly introduced the backdoor into its plant environment during an install or routine software update. The backdoor would not have been detected by a malware scanning kiosk when scanning the portable media or device used to transfer the compromised software package. Once installed in the environment, remotely accessing the backdoor for command and control purposes is mitigated by the defensive architecture. In addition, a licensee would have been made aware of the presence of the backdoor by US-CERT alert AA20-352A, E-ISAC Critical Broadcast Program All-Points Bulletin 20-08, and SolarWinds security advisory and taken corrective action.

When assessing a vulnerability, the licensee should account for how exploitation is possible (i.e., attack vector) because environmental factors that prevent inbound network traffic such as standalone, or air-gapped, networks or use of data diodes limit an attacker's ability to *remotely* exploit certain types of vulnerabilities or take command and control.

Not all exploits accomplish the same end, and an exploit is not an end in and of themselves, except perhaps as proof of concept; they are a means to end (i.e., used to mount a cyber attack).

Ultimately, it's the actions taken by an attacker (or malware) after exploitation occurs, that determines impact to safety, security, and emergency preparedness functions.

5.1 CONSIDERATIONS OF THE DESIGN BASIS THREAT

A *cyber attack* is a deliberate act directed against a nuclear power plant, specifically, against protected assets (digital systems and networks subject to 10 CFR 73.54) to compromise their security. As stated in 10 CFR73.54 (a), cyber attacks that must be protected against are bounded "up to and including" the design basis threat of radiological sabotage. The cyber security defensive architecture is the primary line of defense against nation-state actors and targeted zero-day vulnerabilities.

5.2 ANALYSIS OF SECURITY CONTROLS TO MITIGATE VULNERABILITIES:

Section 3.1, Bullet 2 allows crediting existing controls for vulnerability mitigation,

> "Existing security controls provide protections that may address the applicable attack vectors and exploit associated with a vulnerability".

Per Section 3.1 bullet 3 consider the impact of the vulnerability on existing controls. The standard for if the controls are effective is that they are not,

> "Weakened to the point that adequate defense-in-depth no longer exists to protect the CDAs SSEP function".

Per Section 4.4.3.2,

> "Vulnerabilities that pose a risk to SSEP functions are mitigated when the CAP evaluation concludes remediation is required to maintain adequate defense-in-depth."

6 DETECTION PRIOR TO ADVERSE IMPACT FOR INDIRECT CDAS

During vulnerability analysis of Indirect CDAs the focus is preventing exploitation of a vulnerability that affects detecting the compromise prior to actions being taken to protect the SSEP function.

Indirect CDAs

NEI 13-10, "Cyber Security Control Assessments" states, "Indirect CDAs are those CDAs that cannot have an adverse impact on Safety or Security functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee." For Indirect CDAs, the licensee must also determine "time to detect".

Threat and Vulnerability Management is in scope for Indirect CDAs. However, as with the application of the other controls, it should be consistent with the criteria and potential impact of an Indirect CDA. Detection and response prior to adverse impact along with the baseline

technical controls are the alternate controls required for the technical controls in appendix D and E as well as a limiting factor on other programmatic controls per NEI 13-10, Appendix F. As stated in Section 3.1, previously approved guidance in this addendum allows crediting existing control when they are not weakened by the vulnerability. For Indirect CDAs, consideration is needed if detection as well as the other technical controls specified by NEI 13-10 are weakened by the vulnerability. All other controls are covered per CSP Section 3.1.6.

Vulnerabilities for Indirect CDAs may be evaluated using the same criteria as the basis of the classification of indirect. When it can be shown that a vulnerability does not change the potential impact, time to detect, or compensatory measures, the vulnerability may be considered fully mitigated.

If potential impacts of vulnerabilities can be addressed generically and included in the indirect assessment, then, they need not be considered individually for newly identified vulnerabilities.

When evaluating generic application of mitigations, the following questions and statements should be considered:

- Are any of the required Indirect CDA technical controls weakened to the point that adequate defense-in-depth no longer exists?
    - Per Section 3.1, the control's effectiveness is measured against protection of the CDA's SSEP function, not the CDA.
- Can detection be compromised?
    - Is detection digital or perhaps human?
    - Is detection dependent on an application such as logging, whitelisting, or virus protection?
- Is the Indirect CDA isolated from Direct CDAs by IPS (intrusion protection system) or Firewalls with protection for the protocols used which can limit spread?
    - Does the firewall or IPS limit the communications to known screen-able protocols?
- If detection depends on software or digital infrastructure, can the vulnerability affect the ability to detect compromise?
    - Is the vulnerability in an application such as logging, whitelisting, or virus protection that is depended on for detection or limit the ability of the CDA to run the detection application?
- Does the vulnerability create an unanalyzed means to attack a Direct CDA?
    - Could this vulnerability evade network protections such as HIDS or NIDS which would prevent or slow attacks or access to a Direct CDA?
    - This is not a consideration for isolated CDAs.

(Firewalls, IPS, IDS are at least considerations for determining urgency of patching even if they do not provide specific protocol screening)

7 MAINTAINING DEFENSE-IN-DEPTH

Maintaining defense-in-depth (DID) is a requirement of a licensee's cyber security plan and was codified by the 2009 Power Reactor Security Requirements rulemaking, 10CFR 73.54(c)(2). The NRC delineated specific requirements during the rulemaking period as to how DID is achieved and to clarify the unique differences with DID for 10CFR 73.54 and 10 CFR 73.55, as well as distinguish DID from the traditional design engineering concept of Nuclear Power Plant (NPP) operations.

…The Commission concluded that defense-in-depth for digital computer and communication systems and networks includes technical and administrative controls that are integrated and used to mitigate threats from identified risks…

NEI 08-09 Appendix A, Section 3.1.7 outlines the process for assessing adequate DID measures for applicable attack vectors of CDAs.

7.1 TECHNICAL CONTROLS CONSIDERATIONS FOR EXPLOITATION

The NRC's first area of Cyber Security DID, *Technical Controls*, provides Licensee's with the ability to implement an effective, wide variety of security controls for the mitigation of risks to digital systems. A security control is applied when there is high assurance that CDA is adequately protected and DID is maintained. Cyber Security Technical Controls are in place to support maintaining DID for identified vulnerabilities. Non-networked equipment or isolated trains of equipment help separate the impact, or even the possibility of impact, to an SSEP function if exploited. These technical controls are tools used across all 6 points above to maintain DID and are, in general, new to the NPP operating standards and policies prior to the 2009 Cyber Rule (See Section 7.3 for vulnerability chaining).

7.2 ADMINISTRATIVE CONTROLS USE OF RESTRICTIONS ON LOGICAL ACCESS PERMISSIONS

The NRC's second area of Cyber Security DID, Administrative Controls, provides Licensees with the ability to credit certain organizational protocols that, from a NPP operator perspective, were already in place prior to the Cyber Rule, as well as the development of new administrative controls described in the cyber plan.

Pre-Cyber Rule administrative security protocols, such as Personnel Security and Access Controls, Physical Environment Protection, Vulnerability Management, Monitoring and Maintenance Programs, Configuration and Change Management Programs, Training, Supply Chain Protection and Periodic Program Health Check Polices are all critical in providing the framework by which DID is achieved. Nuclear Power Plant operators have relied on these programs and policies prior to the Cyber Rule and the effectiveness has proven over time to adequately address risks and threats a NPP may incur.

Post-Cyber Rule Administrative Controls such as Cyber Attack Mitigation and Response, Enhanced System and Information Integrity, Media Protection, and Cyber Recovery Plans build upon the already strong NPP administrative infrastructure to further harden against the Design Basis Threat (DBT). In an operating environment, these administrative controls integrate the technical controls into a systematic approach to DID. The exploitation of a vulnerability is further mitigated using these administrative controls, which stretch beyond the immediate capability of a technical control and provide a broader organizational approach managing vulnerabilities.

7.3 FURTHER CONSIDERATIONS FOR VULNERABILITY CHAINING

Note

This section is informational on the concept of vulnerability chaining for consideration when chained vulnerabilities have been identified as exploited. This does not change the requirement to address vulnerabilities with a CVSS score of 7.0 or above for CDAs and a CVSS score of 4.0 and above for defensive architecture.

CVSS User Guide defines and describes the concept of *vulnerability chaining*. Vulnerability chaining is the sequential exploitation of multiple vulnerabilities to attack an IT system, where one or more exploits at the end of the chain require the successful completion of prior exploits to be exploited. Identified vulnerabilities that, if exploited, could expose, or directly impact another vulnerability, should be evaluated, and analyzed as a singular exploitation impact. Whereas vulnerabilities that have no direct impact to each other may be evaluated individually. Chaining vulnerabilities should be an element of vulnerability management assessments. A vulnerability should be considered based on its potential as a gateway to a CDA with adjacent vulnerabilities to a local attack vector.

If a vulnerability can, be exploited only after other preconditions are met (such as first exploiting another vulnerability), it is acceptable to combine two or more CVSS scores to describe the chain of vulnerabilities by scoring for the least-restrictive Exploitability sub-score metrics and scoring for the most-impactful Impact sub-score metrics.

For example, consider VMware vulnerabilities CVE-2022-22954 (base score 9.8 / network) and CVE-2022-22960 (base score 7.8 / local). According to US-CERT alert AA-22-138B, in one instance an unauthenticated actor with network access to the web interface leveraged CVE-2022-22954 to execute an arbitrary shell command as a VMware user. The actor then exploited CVE-2022-22960 to escalate the user's privileges to root. The chain of these vulnerabilities has a base score of 9.8. In other words, CVE-2022-22954 has the same severity but CVE-2022-22960 is more severe if exploited remotely via chaining than if locally.

7.4 APPROPRIATE USE OF DEFENSIVE ARCHITECTURE

Licensees should consider the following points to ensure DID is maintained with justification using technical and administrative controls:

- Applied technical security controls or alternate controls

- Non-networked equipment or isolated trains
- Crediting IPS segmentation when the IPS understands the protocol and the segmentations would preserve the SSEP function from a single cyber attack
- Through analysis or If test systems exist consider penetration testing to show the vulnerabilities are not easily exploitable without external tools or resources
- Physical Security – Protected Area, Vital Areas, Locked Cabinets, Key control program
- Use of Critical Group
- Configuration management
- Work control process
- Centralized / local IDS and log monitoring
- Portable media and device program
- Incident response and disaster recovery

The technical and administrative controls implemented by a licensee constructs the comprehensive DID strategy achieving the points noted within the NRC's 2009 Security Rule Statements of Consideration. Managing vulnerabilities occur in numerous ways, including patching to mitigate against any exploitation. In some cases, the evaluation may identify a period when patching may not be the primary method to mitigate the vulnerably due to other technical or administrative controls set forth in a station's DID framework. In these cases, it may be the intent to ultimately patch or replace the system however, licensees may decide to continue with the current configuration until there is a more appropriate time of remediation (e.g., refueling outage, maintenance outage or complete modification is implemented). The breadth of DID provided by the defensive architecture along with awareness and monitoring, may provide a means of demonstrating adequate protection of SSEP functions until vulnerabilities can be addressed using normal site change management processes.

8 EQUIPMENT PAST END OF SUPPORTED LIFE

8.1 USE OF VULNERABILITY SCANS AND EVALUATION OF RESULTS

For equipment beyond the vendor's supported life cycle, vulnerability scans may be used to fulfill the CSP and E.12 requirements. NEI 08-09, states the following:

- Vulnerability assessments or electronic vulnerability scanning of CDAs are performed as described in Appendix E.12, "Evaluate and Manage Cyber Risk," when new vulnerabilities that could affect the cyber security posture of CDAs are identified.

Control E.12 lists the following requirements for selection of a scan tool:

- Enumerating platforms, software flaws, and improper configurations,
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact

Scans must be performed with privileged accounts to ensure thorough scanning. If available, use test or development systems for scanning. If test systems are not available, and scanning is required on production equipment, the 92-day requirement may be extended until the equipment

can be taken off-line (i.e., outages). Considerations for analyzing applicability of vulnerabilities from scans.

Vulnerabilities identified from scanning older, out of support software, may include vulnerabilities that cannot be exploited. For this software, see Section 9 for considerations associated with currently exploited vulnerabilities.

8.2 ADDRESSING VULNERABILITIES FOR END OF LIFE (EOL) EQUIPMENT FOR DIRECT CDAS

Note:
This section addresses only End of Life equipment for Direct CDAs and uses Addendum 2, "Cyber Attack Detection, Response, and Elimination" to NEI 08-09 where eliminating a vulnerability is too high of a risk (e.g., no vendor support) or causes adverse impact to SSEP functions. The use of Addendum 2 for vulnerability management does not preclude the requirement to identify and assess known vulnerabilities to ensure they do not prevent the timely detection and response to cyber attacks as required by 10 CFR 73.54 (e).

See Section 6 for Indirect CDAs.

As Stated in Addendum 2 to NEI 08-09, 10 CFR 73.54(e) requires that the cyber security plan must describe how the licensee will:

I. Maintain the capability for timely detection and response to cyber attacks;
II. Mitigate the consequences of cyber attacks;
III. Correct exploited vulnerabilities; and
IV. Restore affected systems, networks, and/or equipment affected by cyber-attacks.

When considering if a licensee has timely detection, the following questions should be asked:

- Did the licensee place its detection capability along the network pathway(s) at a location where it can detect cyber attacks and permit the licensee to respond and eliminate the cyber attacks before an adverse impact to the SSEP function?

For TVM IDS or IPS placement, consider:
  - Placement between redundant components
  - Network traffic paths, placed between HMI and Server or IO and server
  - A known protocol (to the IDS\IPS) being used such that it can be effectively be inspected

- Are personnel responsible for cyber attack detection trained in accordance with licensee training standards, and are they sensitive to the indications of a cyber attack?
  - Are responders trained on detection indicators?

- Is there capability for near real time indication of attack?
  - Is the CDA connected to a SIEM and it is properly configured to alert on attack indicators?

- Is the IPS/IDS connected to the SIEM.
- Updating one system at a time with protections between redundant systems can be an indicator for zero-day exploits.
- Is signature-based detection maintained and updated?

When near-real time detection of an event is neither possible nor available, a basis is needed for the potential delay. A Direct CDA is directly performing the SSEP function, therefore time to detect must be based on a license-based standard such as a Tech Spec surveillance. See NEI 08-09, Addendum 2, Section 3 for use of existing Programs and Processes for non-real time detection methods.

8.3 CREDIT FOR ALLOWLISTING

Allowlisting does not remove the vulnerability; however, it addresses the ability to exploit vulnerabilities by accessing the system locally and executing code (or executable scripts). In this case locally refers to where the code must run. It includes remote shell or desktop access. It can be considered as part of the remediation of a network or adjacent vulnerability when other measures address network access.

- Allowlisting addresses local exploits of a vulnerability which cannot be exploited without local code execution.
- Allowlisting does not address vulnerabilities which can be exploited by direct user interaction with the vulnerable code.
    - Consider what other restrictions exist on direct user interaction (i.e., user interface vulnerabilities).
- If the vulnerability is in the OS or existing applications, only LOCAL exploitation aspects are being addressed.
- Network layer vulnerabilities exploited remotely are not solely addressed by allowlisting.

Allowlisting must be implemented, configured, and tested in order to be effective in preventing exploitation of a vulnerability (e.g., all executable types are covered by signature, hash, or signed executable, no OS or application directories are excluded).

8.4 MITIGATIONS FOR END-OF-LIFE EQUIPMENT

Consider the following “Short Term Mitigation Strategies” for bridging time to implement longer term solutions, such as system upgrades or longer-term protections.

- Application of the DRE (Detect, Respond to, Eliminate) processes within this section.
- Reference Appendix A, Section 3.1.6 to ensure the controls mitigate the threat / attack vector the control is intended to protect.
- Credit defense-in-depth after the analysis and create additional defense in depth as warranted with measures such as additional physical security, increased monitoring, or additional administrative measures (working in pairs with verification).

Below are the longer-term solutions to consider when implementing protections:

- Installing whitelisting products on older systems can typically support current virus protection.
- Adding additional detection, such as custom applications which monitor running processes and send SIEM alerts.
- Add network segmentation between redundant systems. If using a firewall with IPS/IDS functionality, then credit it for protection of the SSEP function against network vulnerabilities.
- Determine if the platform can be upgraded, hardware and OS, without a system upgrade. Current Operating Systems are more versatile in their ability to run applications developed for legacy OS than they used to be.
- Consider emulation tools to allow update of the OS for example, Microsoft created a toolkit to allow Windows CE to run on Windows 10 and 11.

9 IMPLEMENTATION OF REMEDIATION

Remediation is the act of correcting a vulnerability *or* mitigating a threat. Three ways of correcting a vulnerability are installing a patch, adjusting configuration settings, or uninstalling a software application. Threats are mitigated by strategically allocating security controls so that adversaries have to overcome multiple (two or more) safeguards to achieve their objective (i.e., a cyber attack per 10 CFR 73.1). Requiring adversaries to defeat multiple mechanisms increases "adversary work factor" (makes it more difficult, not impossible, to exploit a vulnerability to compromise the security of a protected asset) and increases the likelihood of detection.

A licensee might be unable to correct a vulnerability for various reasons (e.g., risk of interruption to plant operations, lack of vendor support, end of product lifecycle/obsolescence). In this case, the focus should be on prevention and detection to accomplish threat mitigation.

It is assumed a licensee has already screened vulnerabilities against its inventory of software and hardware in accordance with the guidance in this Addendum to determine whether they are applicable to their environment.

The subsequent assessment may contain the following based on the licensee's Corrective Action Program:

- Document, if applicable, whether the unmitigated vulnerabilities are exploitable;
- Document how these vulnerabilities will be corrected, or;
- If not correcting unmitigated vulnerabilities:
    - Identify other measures that would prevent vulnerability exploitation,
    - Detect attempts to exploit vulnerabilities,
    - Detect exploited vulnerabilities, or;

- Other detect and delay actions taken by the licensee after exploitation and document these measures and why they provide adequate defense-in-depth.

Licensees shall evaluate attack vectors that are applicable in attempting to exploit the vulnerability.

The attack vector value can be easily determined from the CVSS vector string (a text representation of a set of CVSS metrics commonly used to record or transfer CVSS metric information in a concise form). An attack vector reflects the context by which vulnerability exploitation is possible. CVSS identifies four possible values for attack vector: network, adjacent, logical, and physical. A vulnerability is assigned only one of these values.

A licensee should consider and document where (physically and logically) within its environment an affected component resides and whether the vulnerability can be exploited in its current configuration. Some vulnerabilities might require certain preconditions be met to be exploited. Any preconditions shouldn't be a reason to conclude a vulnerability isn't exploitable but should be used later in the assessment to identify pertinent measures that will prevent and detect a vulnerability from being exploited.

If a remotely exploitable vulnerability (attack vector is "network") affects a critical digital asset connected to an isolated (air-gapped or behind a data diode) network, then a licensee should consider the attack vector to be "adjacent" (limited at the protocol level to a logically adjacent topology such as a local area network).

If, following the analysis of the vulnerability, it is determined that a vulnerability is mitigated, then explain how.

If remediation is required because the controls in place are unable to detect and prevent the vulnerability, then the license should document any corrective actions being taken. Recall from above, correcting a vulnerability is the best approach to prevent exploitation. Another option to consider is applying a workaround, if available.

- Elimination includes any way to correct the vulnerability on the CDA (e.g., patch, remove, change configuration).

- Detection and prevention include updating and validating attempts at exploitation of the vulnerability would be flagged by anti-virus, software integrity, network detection systems, or other detection systems (e.g., update signatures, apply/enable intrusion detection rules).

When detection is relied upon, it shall be expected that a documented time for prevention would be established. The documentation may be through a business plan, Condition Report action, or another long-range plan identifier to share with stakeholders for the next available opportunity to address prevention of the exploit. This would be a future upgrade, install, or replacement that would eliminate the vulnerability. If no such plan exists, then documenting that no such plan exists should be a part of the assessment and understood by the owners.

10 ADDRESSING TVM WITH VENDORS – PO/SPEC REQUIREMENTS FOR EQUIPMENT UPGRADES

10.1 EVALUATING A VENDORS TVM PROGRAM

The NVD (National Vulnerability Database) is the U.S. government repository of standards-based vulnerability management data that can be used to identify vulnerabilities. Utilities use this database as an awareness tool for identifying vulnerabilities and potential impacts to CDA functions and supported equipment within the OT (Operational Technology) environment. While Government Suppliers have begun to understand the importance of vulnerability management programs, many suppliers and system integrators have not. Many control system vendors expect their systems to be isolated or firewall protected and may not patch. Most have a vulnerability management program; however, it may not be adequate in identifying the potential impacts associated with the exploitable vulnerabilities.

To evaluate the adequacy of a proposed vendor program, consider the following questions:

- Who are the system integrator's suppliers? Do the suppliers have a TVM program?
- A TVM evaluation must include every product the vendor installs. Check versions and lifecycles of everything including less obvious products such as backup software which typically runs with high privileges.
- Does the system integrator, including all suppliers, report vulnerabilities to NVD?
    - Do CVEs (Common Vulnerabilities and Exposures) have enough information to be scored? (Not just the vendor supplied score)
    - Do the CVEs typically contain work arounds (options other than patching)?
    - Is there enough information supplied for you to evaluate the potential impact to the function vs risk of exploiting the vulnerability?
    - Reporting to NVD isn't enough. Does the vendor and product appear on NVD's CPE (Common Platform Enumeration) list? The CPE list is how a product can be tied to products used or included in the base product.

10.2 PURCHASE ORDERS AND SPECS

System integrators see it as more cost effective to continue to use a platform or OS, if possible, rather than absorb the cost of redesign. Because of this, accepting a vendor's "standard product" frequently yields soon to be out of support products.

To ensure a PO or Spec contains enough requirements for purchasing a supported product, consider the following:

- Require that all operating systems and installed software shall be within the original suppliers supported life plus no less 3 years.

- Many manufacturers have long term support options. For example, some builds of most Windows products are part of the long-term support channel which guarantees at least a 5-year supported life. Depending on where in the windows lifecycle your purchase is, it can be up to 10 years. Request those builds when possible.
- If network equipment is required, ensure the PO requires managed network equipment. Monitoring increasing the case for detection which helps extend the equipment life.
- On redundant system ask for IPS between systems. This adds detection plus preventing adverse impact and also reduces the need for patching and extends equipment life.
- Whitelisting rather than signature-based products have longer supported product lifecycles. Place your signature-based detection on the network.

Require aggressive and well documented hardening by the integrator. While this is only a requirement on the Direct CDAs hardening reduces the need for patching.