NEI 08-09 [Rev. 6]

Cyber Security Plan for Nuclear Power Reactors

April 2010

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

NEI 08-09 [Rev. 6]

Nuclear Energy Institute

Cyber Security Plan for Nuclear Power Reactors

April 2010

Nuclear Energy Institute, 1776 I Street N. W., Suite 400, Washington D.C. (202.739.8000)

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
Sandra Bittner	Arizona Public Service Company
Cynthia Broadwell	Progress Energy
Steve Carr	Florida Power & Light Company
Larry Cerier	Exelon Corporation
Jeff Drowley	Exelon Corporation
Nathan Faith	American Electric Power Company
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
William Gross	NEI
Glen Kaegi	Exelon Corporation
Tony Lowry	Ameren Corporation
Brian Miller	Progress Energy
Phil Prugnarola	Florida Power & Light Company
Jack Roe	NEI
Ron Rose	FirstEnergy Corporation
Geoff Schwartz	Entergy
Douglas Walker	Exelon Corporation
Brad Yeates	Southern Nuclear Operating Company

NOTICE

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.

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 6 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.

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 6, is contained in Appendix B of NEI 08-09, Revision 6.

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 at all times.
(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 6, 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, Appendix G.

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 6 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 6 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 6 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 6.
- 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 6, Appendix B, Glossary for definition of Critical System)
- Identifies and documents Critical Digital Assets (CDAs). (Refer to NEI 08-09, Revision 6, 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 table top 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 6 consistent with the process described below; and

- Operational and Management cyber security controls in Appendix E of NEI 08-09, Revision 6 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. When a cyber security control is determined to have an adverse effect, alternate controls are used to mitigate the lack of the security control for the CDA per the process described in this section.

For CDAs, the information in Sections 3.1.3 - 3.1.5 is utilized to analyze and document one or more of the following:

1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.
2. Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) above by:
    a. Documenting the basis for employing alternative countermeasures;
    b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control; and
    c. Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control;
    d. Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:
        i. NRC Regulations, Orders
        ii. Operating License Requirements (e.g., Technical Specifications)
        iii. Site operating history
        iv. Industry operating experience
        v. Experience with security control
        vi. Guidance in generally accepted standards (e.g., NIST, IEEE, ISO)
        vii. Audits and Assessments
        viii. Benchmarking
        ix. Availability of new technologies.
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.

3.2 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 6. 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 6, 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 6, 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 with in 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 6, 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 in Levels 4 and 3.
- 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 6, 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 6, 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.
- Security CDAs are in Levels 4 and 3.
- CDAs within a particular security level may not share a common network.
- Safety CDAs are isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air-gaps).
- Security CDAs are isolated from all other CDAs by a defensive boundary that implement the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 6, Appendix E, Section 6.
- 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 6, 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 6.

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 6. 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 6; 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 6, 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 6.

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 6, 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 6, 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 6, 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 6, 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 6, 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 of the physical security program, security plans,

implementing procedures, cyber security programs; safety/security interface activities; the testing, maintenance, and calibration program as it relates to cyber security; and feedback from the NRC and local, state and federal law enforcement authorities.

The effectiveness evaluation provides information for cyber security decision makers about the results of previous policy and acquisition decisions. These measures:

- 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 6;
- Assist in ascertaining whether specific cyber security controls are functioning and are helping facilitate corrective action prioritization; and
- Require fusing the Cyber Security Program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be tied to cyber security control implementation.

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 6, 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 Scans

Electronic vulnerability scanning of CDAs is performed when security controls are first applied, and as required by specific guidance in the cyber security controls in Appendices D and E of NEI 08-09, Revision 6. When new vulnerabilities that could affect the cyber security posture of CDAs are identified, vulnerability scanning will be performed.

Vulnerability scan reports are analyzed and vulnerabilities that could result in a risk to SSEP functions at the site are remediated. Information obtained from the vulnerability scanning process is shared with appropriate personnel to ensure that similar vulnerabilities that may impact interconnected or similar CDA(s) are understood, evaluated and mitigated.

When there is a risk of operational disruption, electronic vulnerability scans are conducted during periods of scheduled outage. Test beds and vendor maintained environments may be used for or in substitution for performing vulnerability scans.

Assessment and scanning process must not adversely impact SSEP functions. If this could occur, CDAs are removed from service or replicated (to the extent feasible) before

assessment and scanning is conducted. If vulnerability assessments or scanning cannot be performed on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls (e.g., providing a replicated system or CDA to conduct scanning) are employed.

A vulnerability assessment may be used as a substitute for vulnerability scanning where there is risk of an adverse impact to SSEP functions, and when off-line, replicated, or vendor test beds are not available. When new vulnerabilities are discovered, the vulnerability assessment considers the same threat vectors as the identified vulnerabilities. When vulnerability assessments are used to verify security controls, the assessment targets the threat vectors the security controls address. In both cases, the vulnerability assessment verifies that the vulnerability or threat vector is addressed to provide high assurance of adequate protection that SSEP functions are protected from cyber attacks up-to and including the Design Basis Threat.

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 6, 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, Appendix G.

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 6, 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 6, 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 6. 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. 0, January 2010
5. Webster's dictionary

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

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.

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.

[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 6, 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 CDA accounts at least every 31 days.
- Requiring access rights to be job function based.
- Conducting reviews when as individuals job function changes to ensure that rights remain limited to the individuals job function.
- Employs computerized mechanisms that support CDA account management functions. The CDA will automatically:
  - Terminate temporary, guest, and emergency accounts within a maximum time period of inactivity at least every 31 days.
  - Disable inactive accounts within 31 days.
  - Create and protect audit records for account creation, deletion and modification,
  - Document and notify system administrators of account creation, deletion and modification activities. This is to make system administrators aware of any account modifications and can investigate potential cyber attacks.

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 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:

- 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 where a CDA cannot support System Use Notifications.

1.9 PREVIOUS LOGON NOTIFICATION

This Technical cyber security control:

- Configures CDAs, upon successful logon, to display the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

- Administratively requires end users to report any suspicious activity to the Cyber Security Program Manager.

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

This Technical cyber security control:

- Documents, supervises, and reviews the activities of users with respect to the enforcement and usage of access controls.
- Employs automated mechanisms within CDAs to support and facilitate the review of user activities.

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

This Technical cyber security control ensures hard and soft copy information in storage, in process, and in transmission is labeled.

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:

- Documents and takes additional precautions to protect networks and bus communications from unauthorized access where protocols lack security controls.
- 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.
- Prohibits the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions.
- 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 for unauthorized wireless access points in accordance with this document and disables access points if unauthorized access points are discovered.
- Conducts scans every 31days for unauthorized wireless access points in accessible areas in accordance with this document and disables access points if unauthorized access points are discovered.

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 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, 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:

- Ensures CDAs provide a warning when allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity, which is based on the function of how quickly storage capacity is consumed, and documents the organization's resources and response times.
- Ensures justification and details of alternate compensating security controls are documented where a CDA cannot respond to audit processing failures.
- Responses to audit failures include the use of an external system to provide these capabilities.
- If audit processing capabilities fail for a CDA or security boundary device, the following occurs:
  - Alerts are sent to designated officials in the event of an audit processing failure.
  - Auditing failures are treated as a failure of the CDA or security boundary device
  - Ensures CDAs with auditing failures take the following additional actions:
    1. Shut down the CDA,
    2. Failover to a redundant CDA, where necessary to prevent adverse impact to safety, security or emergency preparedness functions,
    3. Overwrite, when necessary, the oldest audit record(s), and
    4. Stop generating audit records.

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, 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.
- Configures CDAs to employ underlying hardware separation mechanisms to facilitate security function isolation.
- Configures CDAs to isolate critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and other security functions.
- Configures CDAs to minimize the number of non-security functions included within the isolation boundary containing security functions.
- Configures CDAs security functions as independent modules that avoid unnecessary interactions between modules.
- Configures CDAs security functions as a layered structure minimizing interactions between levels of the design and avoid any dependence by lower levels on the functionality or correctness of higher levels, or
- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support security function isolation 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.

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

This Technical cyber security control configures CDAs to limit the use of resources by priority thus preventing lower-priority processes from delaying or interfering with the CDAs servicing of any higher-priority process.

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

This Technical cyber security control configures CDAs and consoles to employ processing components that have minimal functionality and data storage.

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

This Technical cyber security control employs diverse information technologies in the implementation of CDAs.

3.21 FAIL IN KNOWN (SAFE) STATE

This cyber security control ensures the following:

- CDAs fail in a state that ensures that SSEP functions are not adversely impacted by the CDA's failure, and
- A loss of availability, integrity, or confidentiality, in the event of a failure of the CDA or a component of the CDA is prevented.

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 6, 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 6, 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 AND OPERATIONAL ENVIRONMENT PROTECTION

5.1 PHYSICAL AND OPERATIONAL ENVIRONMENT PROTECTION POLICIES AND PROCEDURES

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 and operational 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 and operational environment protection policy and associated physical and operational environmental 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 & ENVIRONMENTAL 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 and to prevent degradation of the operational environment which could impact the correct performance of CDAs (e.g., by temperature, humidity, dust, vibration, and electromagnetic interference or radio frequency interference).

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 higher security levels to lower security levels.
- 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 6.
- 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 from networks or systems existing at the lower security level to networks or systems existing at the higher security 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 every 12 months.
- 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 every 12 months, 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 by the no less than every 31 days 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 every 92 days.

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 every 92 days, 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 every 92 days, 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:

- Scan or assess for vulnerabilities in the CDAs no less frequently than every 92 days, and at random intervals, and as necessary when new vulnerabilities affecting the CDAs are identified and reported;
- 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.