APPENDIX A

GENERIC CYBER SECURITY PLAN TEMPLATE

[SITE] CYBER SECURITY PLAN

A.1 INTRODUCTION

The purpose of this [Licensee/Applicant] Cyber Security Plan (the plan) is to describe how the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks" (the rule) are implemented to protect digital computer and communications systems and networks associated with the following functions from those cyber attacks, up to and including the design-basis threat (DBT) described in 10 CFR 73.1, "Purpose and Scope":

- safety-related and important-to-safety functions,
- security functions,
- emergency preparedness functions, including offsite communications, and
- support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

As required by 10 CFR 73.54(e) and 10 CFR 73.55(c)(6), licensees and applicants must establish, implement, and maintain a cyber security plan. This plan establishes the licensing basis for the [Licensee/Applicant] Cyber Security Program (the program) for [Site(s)]. [Elements of the program described in this plan are applicable to all sites unless otherwise stated.] [Licensee/Applicant] acknowledges that the implementation of this plan does not alleviate [Licensee/Applicant]'s responsibility to comply with other NRC regulations.

[Licensee/Applicant] complies with the requirements of 10 CFR 73.54 by implementing Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities." RG 5.71 provides a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for complying with this regulation. RG 5.71 includes a glossary of terms that are used within this plan.

A.2 CYBER SECURITY PLAN

A.2.1 Scope and Purpose

This plan describes how [Licensee/Applicant] [will establish/established] a cyber security program to achieve high assurance that [Site] digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions, hereafter defined as critical digital assets (CDAs), are adequately protected against cyber attacks up to and including the DBT. The following actions provide high assurance of adequate protection of systems associated with the above functions from cyber attacks:

- implementing and documenting the "baseline" security controls described in Section 3.3 of RG-5.71, and
- 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 document.

A.2.2 Performance-Based Requirements

As required by 10 CFR 73.55(a)(1), a licensee must implement the requirements of this section through its Commission-approved physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan, referred to collectively as "security plans." As defined in 10 CFR 73.54(b)(3), cyber security is a component of the physical protection program. As such, this plan establishes how [Site] digital computer and communication systems and networks within the scope of 10 CFR 73.54 will be adequately protected from cyber attacks up to and including the DBT.

A.3 CYBER SECURITY PROGRAM IMPLEMENTATION

The [Licensee/Applicant] established and maintains a cyber security program that complies with the requirements of 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8) to protect those systems within the scope of 10 CFR 73.54(a)(1)(i–iv) that can, if compromised, directly or indirectly have an adverse impact on the SSEP functions of a nuclear facility. This cyber security program complies with 10 CFR 73.54 by (1) establishing and implementing defensive strategies consistent with the defensive model described in Section 3.1.5 of this document, including the security controls described in Sections 3.1, 3.2, and 3.3, and (2) maintaining the program, as described in Section 4 of this document.

Documentation of the security controls in place for each CDA is available for inspection. Modifications to the cyber security plan are conducted in accordance with 10 CFR 50.54(p). As required by 10 CFR 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit," [Licensee/Applicant] will submit changes that are determined to decrease the effectiveness of this plan or for any other reason to the NRC for approval. [Licensee/Applicant] will also report any cyber attacks or incidents at [Site] to the NRC, as required by 10 CFR 73.71, "Reporting of Safeguards Events," and Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73, "Physical Protection of Plants and Materials."

A.3.1 Analyzing Digital Computer Systems

A.3.1.1 Security Assessment and Authorization

[Licensee/Applicant] developed and [annually] reviews and updates the following:

- a formal, documented security planning, assessment and authorization policy that describes the purpose, scope, roles, responsibilities, management commitments, and coordination among [Licensee/Applicant] [departments] and the implementation of this cyber security program, the controls in Appendices B and C to RG 5.71, and
- a formal, documented procedure to facilitate the implementation of the cyber security program and the security assessment.

A.3.1.2 Cyber Security Team

[Licensee/Applicant] established and maintains a cyber security team (CST) 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. Individuals with knowledge of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant information systems, are included. Plant operational systems include programmable logic controllers, control

systems, and distributed control systems. Information systems include computer systems and databases containing information used in the design, operation, and maintenance CDAs. The networking arena includes knowledge of both site- and corporate-wide networks.

- Nuclear facility operations, engineering, and safety—This includes overall facility operations and plant technical specification compliance. [Licensee/Applicant] staff representing this technical area trace the impact of a potential vulnerability or series of vulnerabilities in a CDA (or connected digital asset) outward through plant systems and subsystems to ensure that the overall impact on the SSEP functions of the plant is 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 CST include the following:

- performing or overseeing each stage of the cyber security management processes;
- documenting all key observations, analyses, and findings during the assessment process so that this information can be used in the application of security controls;
- evaluating or reevaluating assumptions and conclusions about current cyber security threats; potential vulnerabilities to, and consequences from, an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; and cyber security awareness and training of those working with, or responsible for, CDAs and cyber security controls throughout their system life cycles;
- confirming information acquired during reviews by conducting comprehensive walkdowns of CDAs and connected digital assets and associated cyber security controls, including walkdown inspections with physical and electronic validation activities;
- identifying and implementing potential new cyber security controls, as needed;
- preparing documentation and overseeing implementation of the cyber security controls provided in Appendices B and C to RG 5.71, documenting the basis for not implementing certain cyber security controls provided in Appendix B to RG 5.71, or documenting the basis for the implementation of alternate or compensating measures in lieu of any cyber security controls provided in Appendix B to RG 5.71; and
- assuring the retention of all assessment documentation, including notes and supporting information, in accordance with 10 CFR 73.55(q) and the record retention requirements specified in Section 5 of this plan.

The CST conducts objective security assessments, makes [determinations] that are not constrained by operational goals, and resolves these issues using the process described in Section 3.1.6 of this plan.

A.3.1.3 Identification of Critical Digital Assets

To identify the CDAs at [Site], [Licensee/Applicant]'s CST:

- Identified and documented plant systems, equipment, communication systems, and networks that are associated with the SSEP functions described in 10 CFR 73.54(a)(1), as well as the support systems associated with these SSEP functions. These systems are hereafter referred to as critical systems (CSs). The CST identified CSs by conducting an initial consequence analysis of [Site] plant systems, equipment, communication systems, and networks to determine those which, if compromised, exploited, or failed, could impact the SSEP functions of the nuclear facility, without taking into account existing mitigating measures. For those support systems or

equipment that are associated with SSEP functions, [Licensee/Applicant] performed a dependency and pathway analysis to determine whether those systems or equipment are CSs.

- Identified and documented CDAs that have a direct, supporting, or indirect role in the proper functioning of CSs.

For each CS examined, the [Licensee/Applicant] documented the following:

- a general description of each system, asset, or network identified as a CDA
- the identification of CDAs within each CS
- a brief description of the function provided by each CDA
- an analysis that identifies the potential consequence to both the CS and the SSEP functions if a compromise of the CDA were to occur
- the identification of the digital devices that have direct or indirect roles in the function of the CDA (e.g., protection, control, monitoring, reporting, or communications)
- security functional requirements or specifications 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; and
  - 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,
  - user responsibilities in maintaining the security of the CDA

A.3.1.4 Reviews and Validation Testing

[Licensee/Applicant]'s CST conducted a review and performed validation activities and for each CDA, the CST:

- its direct and indirect connectivity pathways,
- infrastructure interdependencies, and
- the application of defensive strategies, including defensive models, security controls, and other defensive measures.

The CST validated the above activities through comprehensive walkdowns which included:

- performance of a physical inspection of the connections and configuration of each CDA; including tracing all communication connections into and out of the CDA to each termination point along all communication pathways;
- examination of the physical security established to protect each CDA and its communication pathways;
- examination of the configuration and assessment of the effectiveness of existing security controls (e.g., firewalls, intrusion detection systems, diodes) along the communication pathways;
- examination of each CS and/or CDA's interdependencies with other CS and/or CDAs and trust relationships between the CS and/or CDAs;

- examination of the interdependencies with infrastructure support systems, emphasizing potential compromises of electrical power, environmental controls, and fire suppression equipment;
- examination of systems, networks, and communication systems and networks that are present within the plant and could be potential pathways for attacks; and
- resolution of CDA and CS information and configuration discrepancies identified during the reviews, including the presence of undocumented or missing connections, and other cyber security-related irregularities associated with the CDA.

The CST performed an electronic validation when physical walkdown inspections were impractical to trace a communication pathway fully to its conclusion. The team used only electronic validation methods that provide connection validation equivalent to, or better than, physical walkdowns (e.g., use of a digital voltage meter, physical continuity validation).

A.3.1.5 Defense-in-Depth Protective Strategies

[Licensee/Applicant] implemented, documented, and maintains a defense-in-depth protective strategy to ensure the capability to detect, respond to, and recover from cyber attacks on CDAs. The defensive strategy consists of security controls implemented in accordance with Section 3.1 of this plan and the defensive model described in Section 3.2 of RG 5.71, defense-in-depth in Appendix C Section 6, detailed defense architecture of Appendix C Section 7, and maintains the cyber security program in accordance with in Section 4 of Appendix A. The defensive model employed at the site establishes the logical and physical boundaries between CDAs with similar security risks and CDAs with lower security risks.

A.3.1.6 Application of Security Controls

[Licensee/Applicant] established defense-in-depth protective strategies by implementing and documenting the following:

- the defensive model described in Section 3.2 of RG 5.71,
- the physical and administrative security controls established by the [Site] Physical Security Program and physical barriers, such as locked doors, locked cabinets, and locating CDAs in the [Site] protected area or vital area, which are part of the overall security controls used to protect CDAs from attacks,
- the operational and management controls described in Appendix C to RG 5.71 and verification of their effectiveness for each CDA, and
- the technical controls described in Appendix B to RG 5.71 consistent with the process described below.

With respect to technical security controls, [Licensee/Applicant] used the information collected in Section 3.1.4 of this plan to conduct one or more of the following for each CDA:

- implementation of all of the security controls specified in Appendix B to RG 5.71
- for a security control that could not be applied, implementation of alternative controls that eliminate threat/attack vectors associated with one or more of the security controls enumerated in Appendix B to RG 5.71 by:
  - documenting the basis for employing alternative countermeasures
  - performing and documenting an attack vector and attack tree analysis of the CDA and alternative controls to confirm that the countermeasures provide the same or greater protection as the corresponding security control identified in Appendix B to RG 5.71
  - ensuring that the alternative controls provide at least the same degree of protection as the corresponding security control identified in Appendix B to RG 5.71

- not implementing one or more of the security controls enumerated in Appendix B to RG 5.71 by:
  - performing an attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented
  - documenting that the attack vector does not exist (i.e., is not applicable), thereby demonstrating that those specific security controls are not necessary

[Licensee/Applicant] did not apply a security control when it was determined that the control would adversely impact SSEP functions. When a security control was determined to have an adverse effect, then alternate controls were used to mitigate the lack of the security control for the CDA in accordance with the process described above.

[Licensee/Applicant] performed an effectiveness analysis, as described in Section 4.1.2, and vulnerability assessments/scans, as described in Section 4.1.3, of the CDAs to verify that the security program provides high assurance that CDA are adequately protected from cyber attack, up to an including the DBT and has closed any identified gaps.

A.3.2 Incorporating the Cyber Security Program into the Physical Protection Program

Chapter 23 of the physical security plan references the [Site] Cyber Security Program, in accordance with 10 CFR 73.54(b)(3), 10 CFR 73.55(a)(1), and 10 CFR 73.55(c)(6). [Licensee/Applicant] also considered cyber attacks during the development and identification of target sets, as required by the Physical Security Program and 10 CFR 73.55(f)(2).

[Licensee/Applicant] integrated the management of physical and cyber security as follows:

- established a unified security organization which incorporates both cyber and physical security and is independent from operations,
- documented physical and cyber security interdependencies,
- developed policies and procedures to integrate and unify management and physical and cyber security controls,
- incorporated unified policies and procedures to secure CDAs from attacks up to and including the DBT,
- coordinated acquisition of physical or cyber security services, training, devices, and equipment,
- coordinated interdependent physical and cyber security activities and training with physical and cyber security personnel,
- integrated and coordinated incident response capabilities with physical and cyber incident response personnel,
- trained senior management regarding the needs of both disciplines, and
- periodically exercise the entire security organization using realistic scenarios combining both physical and cyber simulated attacks.

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

A.3.3 Policies and Implementing Procedures

[Licensee/Applicant] developed policies and implementing procedures to meet the security control objectives provided in Appendices B and C to RG 5.71. [Licensee/Applicant] documented, reviewed, approved, issued, used, and revised these policies and implementing procedures as described in Section 4 of this plan. In addition, personnel responsible for the implementation and oversight of the program

report to [Chief Nuclear Officer, Chief Nuclear Operations Officer, Vice President of Nuclear Operations, Vice-President] who is accountable for nuclear plant operation.

[Licensee/Applicant]'s procedures establish the specific responsibilities of the positions described in Section 10.10 of Appendix C to RG 5.71.

A.4 MAINTAINING THE CYBER SECURITY PROGRAM

This section establishes the programmatic elements necessary to maintain security throughout the life cycle of CDAs. [Licensee/Applicant] implemented the elements of this section to maintain high assurance that CDAs associated with the SSEP functions of [Site] are adequately protected from cyber attacks.

[Licensee/Applicant] employs a life cycle approach consistent with the controls described in Appendix C to RG 5.71. This approach ensures that the security controls established and implemented for CDAs are adequately maintained to achieve the site's overall cyber security program objectives. For proposed new digital assets, or existing digital assets that are undergoing modification, [Licensee/Applicant] implements the process described in Section 4.2 of this plan.

[Licensee/Applicant] maintains records in accordance with Section 5 of this plan.

A.4.1 Continuous Monitoring and Assessment

[Licensee/Applicant] continuously monitors security controls consistent with Appendix C to RG 5.71. Automated support tools are also used, as appropriate, to accomplish near real-time cyber security management for CDAs. The continuous monitoring program includes the following:

- ongoing assessments to verify that the security controls implemented for each CDA remain in place throughout the life cycle,
- verification that rogue assets have not been connected to the infrastructure,
- periodic assessments of the need for and effectiveness of the security controls identified in Appendices B and C to RG 5.71, and
- periodic 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 manage configuration changes of CDAs. Continuous monitoring may require periodic updates to the cyber security plan.

A.4.1.1 Periodic Assessment of Security Controls

[Licensee/Applicant] performs periodic assessments to verify that the security controls implemented for each CDA remain robust, resilient, and effective in place throughout the life cycle. The CST verifies the status of these security controls [on at least an annual basis] or in accordance with the specific requirements for each security control, as described in Appendices B and C to RG 5.71, whichever is more frequent.

A.4.1.2 Effectiveness Analysis

The CST monitors and measures the effectiveness and efficiency of the Cyber Security Program and the security controls to ensure that both 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 security program and controls includes, but are not limited to,

periodic testing of the security controls, re-evaluation of the capabilities of the adversaries of the DBT, audits of the Physical and Cyber Security Programs and implementing procedures; safety/security interface activities; the Testing, Maintenance, and Calibration Program; operating experience; and feedback from the NRC and local, State, and Federal law enforcement authorities.

The insights gained from these analyses are used to:

- improve performance and effectiveness of the cyber security program,
- manage and evaluate risk,
- improve the effectiveness of implemented security controls described in Appendices B and C to RG 5.71,
- ascertain whether new security controls are required to protect CDAs from cyber attack,
- to verify that existing security controls are functioning properly and are effective at protecting CDAs from cyber attack, and
- to facilitate corrective action of any gaps discovered in the security program.

The CST verifies the effectiveness of security controls [on at least an annual basis] or in accordance with the specific requirements for each security control, as described in Appendices B and C to RG 5.71, whichever is more frequent. The CST reviews records of maintenance and repairs on CDA components to ensure that CDAs which perform security functions are maintained per recommendations provided by the manufacturer.

A.4.1.3 Vulnerability Assessments and Scans

[Licensee/Applicant]'s CST conducts periodic vulnerability scanning and assessments of the security controls, defensive architecture and of all CDAs to identify security deficiencies. The CST performs assessments of security controls and scans for vulnerabilities in CDAs and the environment [no less frequently than once a quarter] or as specified in the security controls in Appendices B and C to RG 5.71, whichever is more frequent, and when new vulnerabilities that could potentially affect the effectiveness the security program and security of the CDAs are identified. In addition, the CST employs up-to-date vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process.

[Licensee/Applicant]'s CST analyzes vulnerability assessment and scan reports and addresses vulnerabilities that could be exploited to compromise CDAs and vulnerabilities that could adversely impact SSEP functions. The CST shares information obtained from the vulnerability assessment and scanning process with appropriate personnel to ensure that similar vulnerabilities that may adversely impact the effectiveness of the security of interconnected or similar CDAs and/or may adversely impact SSEP functions are understood, evaluated, and mitigated.

[Licensee/Applicant] ensures that the assessment and scanning process does not adversely impact SSEP functions. If this should occur, CDAs will be removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. If [Licensee/Applicant] cannot conduct vulnerability

assessments or scanning 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) will be employed.

A.4.2 Change Control

[Licensee/Applicant] systematically plans, approves, tests, and documents changes to the environment of the CDAs, the addition of CDAs to the environment and changes to existing CDAs in a manner that provides a high level of assurance that the SSEP functions are protected from cyber attacks. During the operation and maintenance life cycle phases, the program establishes that changes made to CDAs use the [design control and configuration management procedures or other procedural processes] to ensure that the existing security controls are effective and that any pathway that can be exploited to compromise a CDA is protected from cyber attacks.

During the retirement phase, the [design control and configuration management procedures or other procedural processes] address safety, reliability, and security engineering activities.

A.4.2.1 Configuration Management

[Licensee/Applicant] has implemented and documented the configuration management controls described in Appendix C, Section 11 to RG 5.71. [Licensee/Applicant] implements a configuration and change management process, as described in Section 4.2 of this plan and Section 11 of RG 5.71, to ensure that the site's Cyber Security Program objectives remain satisfied. [Licensee/Applicant] ensures that modifications to CDAs are evaluated in accordance with Section 4.2 of this plan before any modification is implemented so as to maintain the cyber security performance objectives articulated in 10 CFR 73.54(a)(1).

During the operation and maintenance phases of a CDA life cycle, the [Licensee/Applicant] ensures that changes made are conducted using these configuration management procedures to avoid the introduction of additional vulnerabilities, weaknesses, or risks into the system. This process also ensures timely and effective implementation of each security control specified in Appendices B and C to RG 5.71.

A.4.2.2 Security Impact Analysis of Changes and Environment

[Licensee/Applicant]'s CST performs a security impact analysis in accordance with section 4.1.2 before implementing a design or configuration change to a CDA or when changes to the environment occur so as to manage potential risks introduced by the changes.

[Licensee/Applicant]'s CST evaluates, documents, and incorporates into the security impact analysis safety and security interdependencies of other CDAs or systems, as well as updates and documents the following:

- the location of the CDA and connected assets,
- connectivity pathways (direct and indirect),
- infrastructure interdependencies,
- application of defensive strategies, including defensive models, security controls, and other defensive strategy measures, and
- plantwide physical and cyber security policies and procedures that secure CDAs from a cyber attack, including attack mitigation and incident response and recovery.

[Licensee/Applicant] performs these impact analyses as part of the change approval process to assess the impacts of the changes on the security posture of CDAs and security controls, as described in Section 4.1.2 of this plan, and to address any identified gaps to protect CDAs from cyber attack, up to and including the DBT as described in Section 4.2.6.

[Licensee/Applicant] manages CDAs for the cyber security of SSEP functions through an ongoing evaluation of threats and vulnerabilities and implementation of each of the security controls provided in Appendices B and C to RG 5.71 during all phases of the life cycle. Additionally, [Licensee/Applicant] has established and documented procedures for screening, evaluating, mitigating, and dispositioning threat and vulnerability notifications received from credible sources. Dispositioning includes implementation of security controls to mitigate newly reported or discovered threats and vulnerabilities.

A.4.2.3 Security Reassessment and Authorization

[Licensee/Applicant] has established, implemented, documented, and maintains a process that ensures that modifications to CDAs are evaluated before implementation so that security controls remain effective and that any pathway that can be exploited to compromise the modified CDA is addressed to protect CDAs and SSEP functions from cyber attacks. The program establishes that additions and modifications are evaluated, using a proven and accepted method, before implementation to provide high assurance of adequate protection against cyber attacks, up to and including the DBT, using the process discussed in Section 4.1.2 of this plan.

[Licensee/Applicant] disseminates, reviews, and updates the following when a CDA modification is conducted:

- a formal, documented security assessment and authorization policy which addresses the purpose, scope, roles, responsibilities, management commitment, coordination among [Licensee/Applicant] entities, and compliance to reflect all modifications or additions, and
- a formal, documented procedure to facilitate the implementation of the security reassessment and authorization policy and associated controls.

A.4.2.4 Updating Cyber Security Practices

The [Licensee/Applicant]'s CST reviews, updates and modifies [Site] cyber security policies, procedures, practices, existing cyber security controls, detailed descriptions of network architecture (including logical and physical diagrams), information on security devices, and any other information associated with the state of the security program or security controls provided in Appendices B and C to RG 5.71 when changes occur to CDAs or the environment. This information includes the following:

- plant- and corporate-wide information on the policies, procedures, and current practices related to cyber security;
- detailed network architectures and diagrams;
- configuration information on security devices or CDAs;
- new plant- or corporate-wide cyber security defensive strategies or security controls being developed and policies, procedures, practices, and technologies related to their deployment,
- the site's physical and operational security program;
- cyber security requirements for vendors and contractors;
- indentified potential pathways for attacks;
- recent cyber security studies or audits (to gain insight into areas of potential vulnerabilities); and
- indentified infrastructure support systems (e.g., electrical power; heating, ventilation, and air conditioning; communications; fire suppression) whose failure or manipulation could impact the proper functioning of CSs.

A.4.2.5 Review and Validation Testing of a Modification or Addition of a Critical Digital Asset

The [Licensee/Applicant]'s CST conducts and documents the results of reviews and validation tests of each CDA modification and addition using the process described in Section 3.1.4 of this plan.

A.4.2.6 Application of Security Controls Associated with a Modification or Addition

When new CDAs are introduced into the environment, the [Licensee/Applicant]:

- deploys the CDA into the appropriate level of the defensive model described in Section 3.1.5 of this plan,
- applies the technical controls identified in Appendix B to RG 5.71 in a manner consistent with the process described in Section 3.2 of RG 5.71, and
- confirms that the operational and management controls described in Appendix C of RG 5.71 are applied and effective for the CDA.

When CDAs are modified, the [Licensee/Applicant]:

- verifies that the CDA is deployed into the proper level of the defensive model described in Section 3.2 of RG 5.71,
- performs a security impact analysis, as described in Section 4.2.2 of this plan,
- verifies that the technical controls identified in Appendix B to RG 5.71 are implemented in a manner consistent with the process described in Section 3.1.6 of this plan,
- verifies that the security controls discussed above are implemented effectively, consistent with the process described in Section 4.1.2 of this plan, and
- confirms that the operational and management controls discussed in Appendix C to RG 5.71 are applied and effective for the CDA.

A.4.3 Cyber Security Program Review

[Licensee/Applicant] Cyber Security Program establishes the necessary measures and governing procedures to implement periodic reviews of applicable program elements, in accordance with the requirements of 10 CFR 73.55(m).

[Licensee/Applicant] reviews the program's effectiveness [at least every 24 months]. In addition, reviews are conducted as follows:

- within 12 months of the initial implementation of the program;
- within 12 months of a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security;
- as necessary based upon site-specific analyses, assessments, or other performance indicators; and
- by individuals independent of those personnel responsible for program implementation and management.

[Licensee/Applicant] documents the results and recommendations of program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program review, in a report to the [Site's] [plant manager and to licensee corporate management] at least one level higher than the individual having responsibility for day-to-day plant operation. [Licensee/Applicant] maintains these reports in an auditable form, available for inspection, and enters findings from program reviews into the site's Corrective Action Program.

A.5 DOCUMENT CONTROL AND RECORDS RETENTION AND HANDLING

[Licensee/Applicant] 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. [Licensee/Applicant] will retain records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," until the NRC terminates the facility operating license. Records required for retention include, but are not limited to, all digital records, log files, audit files, and nondigital records that capture, record, and analyze network and CDA events. These records are retained to document access history and discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions or both. [Licensee/Applicant] will retain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the NRC.