U.S. NUCLEAR REGULATORY COMMISSION January 2010

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 5.71

(New Regulatory Guide)

CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES

A INTRODUCTION

Title 10, of the *Code of Federal Regulations,* Section 73.54, "Protection of Digital Computer and Communication Systems and Networks" (10 CFR 73.54) (Ref. 1) requires, in part, that U.S. Nuclear Regulatory Commission (NRC) 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 (DBT), as described in 10 CFR 73.1, "Purpose and Scope."

In particular, 10 CFR 73.54(a)(1) requires licensees to protect digital computer and communications systems and networks associated with the following categories of functions, from those cyber attacks identified in 10 CFR 73.54(a)(2):

- 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.

The NRC issues regulatory guides to describe and make available to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public.

Regulatory guides are issued in 10 broad divisions—1, Power Reactors; 2, Research and Test Reactors; 3, Fuels and Materials Facilities; 4, Environmental and Siting; 5, Materials and Plant Protection; 6, Products; 7, Transportation; 8, Occupational Health; 9, Antitrust and Financial Review; and 10, General.

Electronic copies of this guide and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html under Accession No. ML090340159.

10 CFR 73.54(a)(2) requires the licensee to protect such systems and networks from those cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems, services, or data; and impact the operation of systems, networks, and equipment.

This regulatory guide provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1. Licensees may use methods other than those described within this guide to meet the Commission's regulations if the chosen measures satisfy the stated regulatory requirements.

This regulatory guide applies to operating reactors licensed in accordance with 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 2), and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 3). Licensees and applicants should consider this guidance in preparing an application for a combined operating license under 10 CFR Part 52. Licensees and applicants bear the sole responsibility for assessing and managing the potential for adverse effects on safety, security, and emergency preparedness (SSEP) so as to provide high assurance that critical functions are adequately protected from cyber attacks. Licensees and applicants should direct their questions regarding regulatory requirements for the protection of digital computer and communication systems and networks to the appropriate NRC headquarters or regional office staff.

This regulatory guide contains information collection requirements covered by 10 CFR Part 73 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

TABLE OF CONTENTS

B DISCUSSION

Nuclear power plant licensees' physical protection programs must comply with the performance objectives and requirements outlined in 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." 73.55(b)(8) further requires these licensees to establish, maintain, and implement cyber security program in accordance with 73.54. Incorporating a cyber security program to protect those digital computer and communication systems and networks identified in 10 CFR 73.54(a)(1) into the site physical protection program requires that the high assurance of adequate protection standard for physical protection be applied to the protection of these systems. Specifically, licensees are required to protect the systems identified in 10 CFR 73.54(a)(1) through the establishment and maintenance of an onsite physical protection program and security organization whose objective is to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

In response to the terrorist attacks of September 11, 2001, and subsequent information provided by intelligence and law enforcement agencies, the NRC issued NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," in February 2002 (Ref. 4) to address the threat environment at the time. This order included a specific requirement that directed nuclear power plant licensees to address certain cyber security vulnerabilities.

The NRC issued a subsequent order, EA-03-086, "Design Basis Threat for Radiological Sabotage," in April 2003 (Ref. 5). This order supplemented the Design Basis Threat (DBT) for nuclear power plants as specified in 10 CFR 73.1 and, in part, required licensees to address additional cyber attack characteristics. The material aspects of NRC Orders EA-02-026 and EA-03-086 are withheld from public disclosure in accordance with 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements."

In addition, in recognition of the potential cyber-security-related issues resulting from the increased use of digital technology at nuclear power plants, in October 2004, the NRC published NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants" (Ref. 6). Using NUREG/CR-6847 and insights gained during its development, the Nuclear Energy Institute (NEI) developed NEI 04-04, "Cyber Security Program for Power Reactors," to provide nuclear power reactor licensees with a means for developing and maintaining a cyber security program at their sites. The NRC staff evaluated the NEI submittal and, by letter dated December 23, 2005 (Ref. 7), informed NEI that NEI 04-04, Revision 1, dated November 18, 2005 (Ref. 8), provided an acceptable approach to formulating an interim cyber security program at the time of the NRC's endorsement of NEI 04-04, the NRC had not yet proposed comprehensive cyber security regulations. Although NUREG/CR-6847 provided licensees with information useful for developing an interim cyber security program for their facilities prior to the codification of cyber security requirements, it does not provide an acceptable means for complying with the requirements of 10 CFR 73.54. Instead, for systems within the scope of 10 CFR 73.54, this RG 5.71 provides a comprehensive approach to comply with 10 CFR 73.54 for cyber security, by using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems" (Ref. 9).

In January 2006, the NRC published Regulatory Guide (RG) 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 10). RG 1.152, Revision 2, provided specific guidance to nuclear power plant licensees for use in the design, development and implementation

of protection measures for digital instrumentation and controls employed in safety-related applications. Specifically the guidance addressed those aspects of the implementation of measures within safety systems that were not adequately covered in Institute of Electrical and Electronics Engineers (IEEE) Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," dated September 11, 2003 (Ref. 11). The RG 1.152, Revision 2, contains regulatory criteria for the evaluations of safety systems to ensure that identified security features were appropriately incorporated into systems and that the development environment was protected against the introduction of undocumented, unwanted code and any other coding that could adversely impact operation of the safety system. Any acquisition or modification of digital safety systems or any licensing of new reactor safety systems (one subset of the critical digital assets covered by RG 5.71) are reviewed via a license amendment request or design certification application or combined operating license (COL) application. RG 1.152, Revision 2, regulatory positions 2.1 – 2.9 are used as the basis for the license amendment or design certification or COL review of digital safety systems. If a licensee or applicant chooses to address 10 CFR 73.54 though the use of design features, then details of any design features of the safety system, intended to meet a cyber security provision of 10 CFR 73.54, must be submitted as part of the license amendment request or design certification application or COL application for review and approval. In such cases, the NRC will review those features only in conjunction with the system's safety functions to ensure that the reliability of the safety system is not adversely impacted by the inclusion of these security features.

In March 2007, the NRC released Branch Technical Position (BTP) 7-14, Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," (Ref. 12). BTP 7-14, Revision 5, provided review guidelines for evaluating software life-cycle processes associated with safety-related digital instrumentation and control systems at nuclear power plants. It also addressed the characteristics of an acceptable software management plan.

In 10 CFR 73.55(b), the Commission established requirements for the physical protection program of a nuclear power reactor facility. These include performance criteria for detecting, assessing, interdicting, and neutralizing threats up to and including the DBT of radiological sabotage. As specified in 10 CFR 73.1(a)(1)(v), a cyber attack is a component of the DBT against which a licensee's physical protection program must be able to defend with high assurance.

This regulatory guide provides guidance to applicants and licensees on satisfying the requirements of 10 CFR 73.54. The information contained within this guide represents the results of research conducted by the NRC Office of Nuclear Regulatory Research concerning cyber security program development and the collective body of knowledge and experience that has been developed through all of the actions identified above. In addition, this guide embodies the findings by standards organizations and agencies, such as the International Society of Automation, IEEE, and NIST, as well as guidance from the U.S. Department of Homeland Security (DHS).

RG 5.71 describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in NIST SP 800-53 and NIST SP 800-82, "Guide to Industrial Control Systems Security," dated September 29, 2008 (Ref. 13). NIST SP 800-53 and SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques. Furthermore, NIST developed SP 800-82 for use within industrial control system (ICS) environments, including common ICS environments in which the information technology (IT)/ICS convergence has created the need to consider application of these security controls. RG 5.71 divides the above-noted security controls into three broad categories: technical, operational, and management.

If a cyber attack were to result in the loss or degradation of SSEP functions, the health and safety of the public might be at risk. Consequently, the NRC developed this regulatory guide by tailoring the "high impact" baseline security controls described in NIST SP 800-53 and NIST SP 800-82 to provide an acceptable method to comply with 10 CFR 73.54. Where applicable, the NRC staff tailored the controls in NIST SP 800-53 and SP 800-82 to the unique environments of nuclear facility licensees and provided these more specific controls in Appendices A, B, and C to this document. The NRC's efforts to tailor the NIST baseline security controls are consistent with the recommendations provided in Appendix I to NIST SP 800-53 and in NIST SP 800-82. The process NIST used to develop these security controls was both peer reviewed and open to industry comment, and thus provides a well-established standard for cyber security which licensees should adopt to satisfy the regulatory requirement to defend digital assets from cyber attack up to and including the DBT, as defined in 10 CFR 73.1.

RG 5.71 provides a framework to aid in the identification of those digital assets that must be protected from cyber attacks. These identified digital assets are referred to as "critical digital assets" (CDAs). Licensees should address the potential cyber security risks of CDAs by applying the defensive architecture and the collection of security controls identified in this regulatory guide.

The RG 5.71 framework offers licensees and applicants the ability to address the specific needs of an existing or new system. The goal of this regulatory guide is to harmonize the well-known and well-understood set of security controls (based on NIST cyber security standards) that address potential cyber risks to CDAs to provide a flexible programmatic approach in which the licensee or applicant can establish, maintain, and successfully integrate these security controls into a site-specific cyber security program.

The organization of RG 5.71 reflects the steps necessary to meet the requirements of 10 CFR 73.54 using the template for a generic security plan provided in Appendix A. Specifically, Section C.1, "General Requirements," provides an overview of the regulatory requirements relevant to cyber security. Section C.2, "Elements of a Cyber Security Plan," introduces the elements of a security plan and provides an acceptable method for the development a cyber security plan that will comply with the provisions of 10 CFR 73.54.

Section C.3, "Establishing and Implementing a Cyber Security Program," details an acceptable method for identifying digital assets as CDAs, addressing potential cyber security risks to CDAs and implementing defensive strategies to protect SSEP functions. The compartmentalization and protection of CDAs are key elements in defense-in-depth strategies. As previously discussed, RG 5.71 follows the recommendations of NIST SP 800-53 and 800-82 by providing a list of security controls to address the potential cyber risks to a CDA. Specifically, the NIST standards recommend over 100 security controls, which are categorized into 18 families. These families of security controls are further divided into three classes: technical, operational, and management. Section C.3 also describes an acceptable method for implementing the security controls, as detailed in Appendix B, "Technical Controls," and Appendix C, "Operational and Management Controls," to this guide.

Section C.3 continues guidance associated with policies and procedures needed to address regulatory requirements relating to the implementation of the cyber security program. Policies and procedures are essential parts of security controls, and successful security management planning relies on the existence of properly developed policies and procedures.

Section C.4, "Maintaining the Cyber Security Program," discusses the need to maintain the cyber security program established based on the guidance in Section C.3. CDAs require comprehensive

monitoring of the effectiveness of their security protection measures. A cyber security program must also ensure that changes to the CDAs or the environment are controlled, coordinated, and periodically reviewed for continued protection from cyber attacks. Section C.4 also addresses periodic program review requirements. Lastly, Section C.5, "Records Retention and Handling," provides licensees and applicants with guidance for retaining records associated with their cyber security programs.

Appendix A to RG 5.71 provides a template for a generic cyber security plan which licensees and applicants may use to comply with the licensing requirements of 10 CFR 73.54. Appendices B and C provide an acceptable set of security controls, developed from the NIST cyber security standards and security controls, which are based on well-understood threats, vulnerabilities, and attacks, coupled with equally well-understood and vetted countermeasures and protective techniques.

C REGULATORY POSITION

C.1 General Requirements

Consistent with 10 CFR 73.54(a), a licensee must provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the DBT, as described in 10 CFR 73.1. Consistent with 10 CFR 73.54(a)(1), licensees must protect from cyber attacks digital computer and communication systems associated with certain categories of functions and support systems and equipment, which, if compromised, would adversely impact the SSEP functions of a nuclear facility. These functions include safety-related and important-to-safety functions, security functions, and emergency preparedness functions (including offsite communications). The rule specifies that digital computer and communication systems and networks associated with these functions must be protected from cyber attacks that would adversely impact the integrity or confidentiality of data and software; deny access to systems, services, or data; or provide an adverse impact to the operations of systems, networks, and associated equipment.

C.2 Elements of a Cyber Security Plan

As stated in 10 CFR 73.54(e), the licensee must establish, implement, and maintain a cyber security plan that satisfies the cyber security program requirements of this regulation. In addition, the cyber security plan must describe how the licensee will implement the requirements of the regulation and must account for the site-specific conditions that affect implementation. One method of complying with this regulation is to describe within the cyber security plan how the licensee has achieved high assurance that all SSEP functions are protected from cyber attacks. This section lists the necessary elements of a cyber security plan, as required by the rule.

In accordance with 10 CFR 73.54(e), the cyber security plan must describe how the licensee will implement the requirements of 10 CFR 73.54 at a nuclear facility. To further guide licensees, Appendix A to this RG provides a generic cyber security plan template that can be used to develop a cyber security plan and to establish and maintain a cyber security program that will comply with this regulation.

The cyber security plan describes the measures and governing procedures to ensure that the plan, associated records, and implementing policies and procedures are protected in accordance with the NRC's requirement for protection of safeguard information, as stated in 10 CFR 73.21 and 73.22. Revisions to the cyber security plan must be processed in accordance with 10 CFR 50.54(p). A licensee must submit changes that decrease the effectiveness of the plan to the NRC for approval before their implementation.

As required by 10 CFR 73.54(e)(1), the cyber security plan must describe how the licensee has achieved high assurance that digital systems associated with SSEP functions, including support systems and equipment, are protected from cyber attacks. The cyber security plan must describe the following elements:

- how the licensee provides high assurance that its digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks, up to and including the DBT, as described in 10 CFR 73.1 (10 CFR 73.54(a)(1)):
  - safety-related and important-to-safety functions
  - security functions

  - emergency preparedness functions, including offsite communications
  - support systems and equipment, which if compromised, would adversely impact SSEP functions
- how the licensee protects these systems and networks from cyber attacks that would have the following effects (10 CFR 73.54(a)(2)):
  - adversely impact the integrity or confidentiality of data or software
  - deny access to or adversely impact the availability of systems, services, or data
  - adversely impact the operation of systems, networks, and associated equipment
- the approach to identify CDAs that are within the scope of the rule (10 CFR 73.54(b)(1))
- how the licensee established, implements, and maintains its cyber security program (10 CFR 73.54(b)(2))
- how the licensee has incorporated the cyber security program into the physical security program (10 CFR 73.54(b)(3))
- the security controls used and how they protect the assets identified in 10 CFR 73.54(b)(1) (10 CFR 73.54(c)(1))
- defense-in-depth protective strategies and how they are used to protect, detect, respond to, and recover from cyber attacks (10 CFR 73.54(c)(2))
- the elements of the cyber security program that are designed to mitigate the adverse effects of cyber attacks (10 CFR 73.54(c)(3))
- how the cyber security program is designed to ensure that the functions of protected assets identified by 10 CFR 73.54(b)(1) are not adversely impacted by cyber attacks (10 CFR 73.54(c)(4))
- how the cyber security awareness and training programs (10 CFR 73.54(d)(1)) provide the training necessary to perform assigned duties and responsibilities
- the process used by the licensee to evaluate and manage cyber security risks (10 CFR 73.54(d)(2))
- the controls used within the site configuration management and design control processes to ensure the following (10 CFR 73.54(d)(3)):
  - modifications to plant assets and the addition of new equipment do not adversely impact cyber security
  - cyber security issues are addressed throughout the system design life cycle
  - RG 1.152, Rev. 2 (Ref. 10) provides additional guidance for the design and development process of safety systems
- how the site-specific conditions affect cyber security program implementation (10 CFR 73.54(e)(1))
- the measures for incident response and recovery from cyber attacks, including a description of how the licensee will achieve the following (10 CFR 73.54(e)(2)):
  - maintain the capability for timely detection and response to cyber attacks
  - mitigate the consequences of cyber attacks
  - correct exploited vulnerabilities
  - restore affected systems, networks, and equipment affected by cyber attacks
- the specific cyber security policies and procedures that implement the cyber security plan which must be maintained at the site and are subject to inspection by the NRC (10 CFR 73.54(f))
- how the cyber security program is reviewed as a component of the physical security program, in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements (10 CFR 73.54(g))
- how the licensee manages all records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54(h)

C.3 Establishing and Implementing a Cyber Security Program

The regulations set forth in 10 CFR 73.54 establish an overall performance-based requirement to ensure that the functions of digital computer and communication systems and networks are protected from cyber attack. One method of complying with these regulations is to implement and maintain a cyber security program that consists of the defensive architecture described in Section C.3.2.1 and the security controls provided in Section C.3.3.

As required by 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8), a nuclear power plant licensee must establish, implement, and maintain a cyber security program that protects any digital system, network, or communication system, as delineated by 10 CFR 73.54(a)(1)(i–iv), associated with the SSEP functions of a nuclear facility or which supports such a system. Sections C.3 and C.4 describe an acceptable method for establishing, implementing, and maintaining a cyber security program to comply with the regulations. Figure 1 illustrates the process of establishing, implementing, and maintaining the cyber security program.

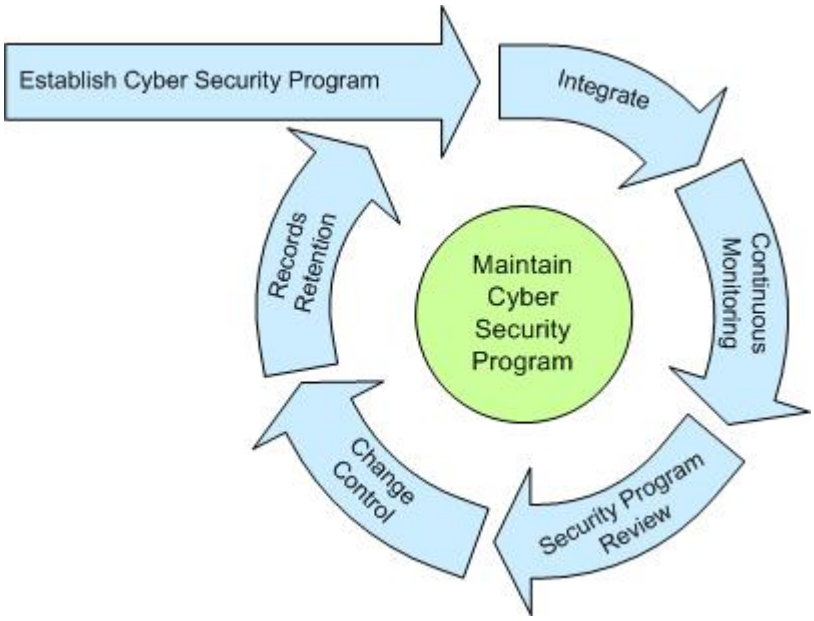

Figure 1 Security life cycle process

An acceptable method to establish a cyber security program at a facility is by performing the following: (1) analyze the digital computer and communication systems and networks, (2) perform a review of the CDAs in Section C.3.1.4, (3) deploy defensive architecture described in Section C.3.2.1, (4) address potential cyber risks to CDAs as described in Section C.3.3, and (5) implement the security life-cycle activities discussed in Section C.4 to maintain the cyber security program.

C.3.1 Analyzing Digital Computer Systems and Networks

Consistent with the requirements of 10 CFR 73.54(b)(1), a licensee must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs, which are those

assets that, if compromised, could adversely impact the SSEP functions of nuclear facilities. An acceptable method for identifying and documenting CDAs is as follows:

- obtain authorization for security assessment,
- define roles and responsibilities cyber personnel and form the cyber security team,
- identify and document CDAs at the facility, and
- review and validate configurations of CDAs.

Section 3.1 of Appendix A to this document provides a template that licensees may follow to describe how they analyzed digital computer systems and networks to identify CDAs.

C.3.1.1 Security Assessment and Authorization

One acceptable method to conduct a process by which an organization allocates people and resources to organize and establish authority and gain commitment to perform a cyber security assessment as the first step in the implementation of the cyber security program is to develop, disseminate, and [annually] review and update the following:

- a formal, documented security assessment and authorization policy that defines and delineates the purpose, scope, roles, responsibilities, management commitments, coordination among licensee departments, and implementation of the security controls described in Appendices B and C to this regulatory guide, and
- a formal, documented procedure to facilitate the implementation of the security assessment.

Section 3.1.1 of Appendix A to this document contains a template for licensees to use in preparing that aspect of their cyber security plan which discusses the security assessment and authorization of the program.

C.3.1.2 Define Roles and Responsibilities and Form the Cyber Security Team

A licensee can form a cyber security team (CST) by defining and documenting roles, responsibilities, authorities, and functional relationships and ensuring that they are understood by site organizations and individuals (including employees, subcontractors, temporary employees, visiting researchers, and vendor representatives) at every level in the organization. An acceptable method for defining the division of responsibility for personnel administering the cyber security program includes the following four categories of individuals:

- a cyber security program sponsor who is a member of senior site management (executive or officer level) and has overall responsibility and accountability for the cyber security program and provides the necessary resources for its development, implementation, or maintenance
- a cyber security program manager who is responsible for the following:
  - overseeing cyber security operations
  - functioning as the single point of contact for all issues related to cyber security
  - providing oversight and direction on issues regarding cyber security
  - initiating and coordinating cyber security incident response team (CSIRT) functions, as required
  - coordinating with the NRC, DHS, U.S. Department of Energy, and Federal Bureau of Investigation, as required, during and after cyber security incidents and events

  - overseeing and approving the development and implementation of a cyber security plan, policies, and procedures
  - ensuring and approving cyber security education, awareness, and training activities
- cyber security specialists who are responsible for the following:
  - protecting CDAs from cyber threats
  - configuring, operating, and maintaining cyber security equipment
  - understanding the cyber security aspects of the overall architecture of plant networks operating systems, hardware platforms, software platforms, operating systems, and applications; plant-specific applications; and the services and protocols upon which those applications rely
  - performing cyber security evaluations of digital systems
  - conducting security audits, vulnerability assessments, network scans, and penetration tests against CDAs,
  - conducting cyber security investigations following the compromise of CDAs
  - preserving forensic evidence collected during cyber security investigations to prevent loss of evidentiary value
  - maintaining expert skill and knowledge in the area of cyber security
  - acting as the primary director or leader of a CSIRT
- a CSIRT composed of individuals from organizations, including security, operations, engineering, emergency preparedness, and other support organizations, as required, which is responsible for the following:
  - initiating appropriate response and actions to protect CDAs from compromise during a known or suspected security incident and assisting with recovery of compromised systems
  - containing and mitigating security incidents involving CDAs and ensuring that compromised systems are properly restored following an incident
- auxiliary staff, including operations personnel, engineers, technicians, users, contractors, and vendor representatives, who operate, maintain, or design digital systems.

An acceptable method to use in forming the CST is to assemble or designate a team 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. The networking arena includes knowledge of both plant- and corporate-wide networks.
- Nuclear facility operations, engineering, and safety—This includes 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 systems and subsystems so that the overall impact on the 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.

Roles and responsibilities of the CST include the following:

- performing or overseeing each stage of the cyber security and management process;
- documenting all key observations, analyses, and findings during the assessment process so that this information can be used as a basis for applying 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; cyber security awareness and training of those working with or responsible for CDAs and cyber security controls throughout their system life cycles; and managing cyber security;
- confirming information acquired during reviews by conducting comprehensive walkdowns of CDAs and connected digital assets, as well as associated cyber security controls, including walkdown inspections with physical and electronic validation activities;
- identifying and implementing potential new cyber security controls;
- preparing documentation and overseeing implementation of the cyber security controls provided in Appendices B and C to this guide, documenting the basis for not implementing certain cyber security controls provided in Appendix B, or documenting the basis for the implementation of alternate or compensating measures in lieu of any cyber security controls provided in Appendix B; and
- assuring the retention of all assessment documentation, including notes and supporting information, in accordance with 10 CFR 73.54(h) and the record retention and handling requirements specified in Section C.5 of this guide.

The licensee's CST needs to have the authority to conduct an objective assessment, make determinations that are not constrained by operational goals (e.g., cost), implement the defense-n-depth protective strategies discussed in Section C.3.2, and ensure the implementation of the security controls using the process described in Section C.3.3 of this document. Section 3.1.2 of Appendix A provides a template which a licensee may use in describing the formation of its CST, and Section 10.10 of Appendix C to this guide outlines the roles and responsibilities that define the division of responsibilities for personnel administering the cyber security program.

C.3.1.3 Identification of Critical Digital Assets

As noted earlier, licensee assets that must be protected from cyber attack under 10 CFR 73.54 are referred to in this document as "critical digital assets" (CDAs). However, it may be difficult for a licensee to identify CDAs without first conducting a wider assessment of all of the systems within the facility. A typical nuclear power plant contains hundreds of individual systems that contribute to the overall operation, safety, and security of the facility. Figure 2 illustrates one generic categorization of plant systems as they are associated with the SSEP functions in a typical nuclear facility. To the extent that these systems are associated with SSEP functions, a compromise of these plant systems could result in radiological sabotage (i.e. significant core damage) and therefore has the potential to adversely impact the public health and safety. Although all of these systems may not ultimately be within the scope of the licensee's cyber security program, the licensee's accurate identification of these plant systems associated with a SSEP function is essential to the development of an effective cyber security program that meets the requirements of 10 CFR 73.54. Once the licensee identifies these systems, the licensee can then use that information to establish the set of equipment that will be protected under its cyber security program. One acceptable method to conduct this analysis is described in following section.

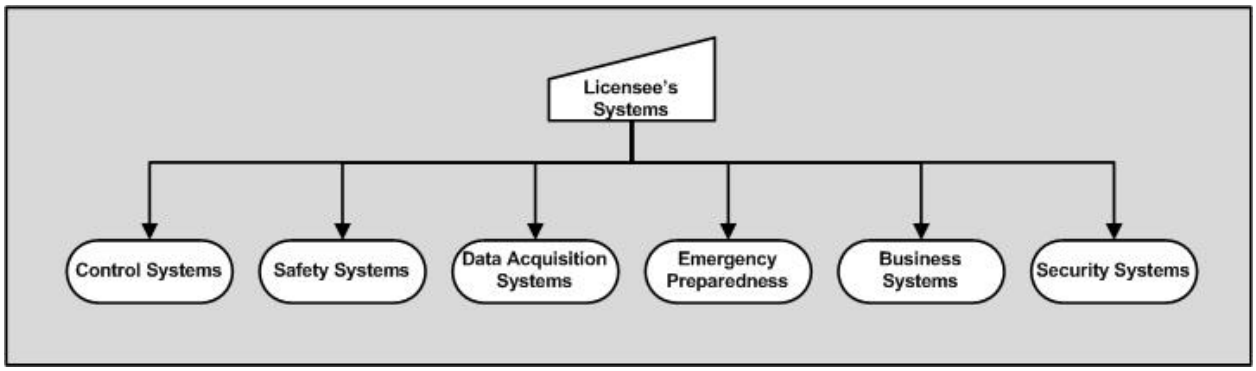

Figure 2 Categorization of plant systems

To identify CDAs, a licensee should first identify the overall allocation and organization of plant systems, equipment, communication systems, and networks that are associated with the SSEP functions or support systems that are associated with SSEP functions. These systems, hereafter broadly referred to as "critical systems" (CSs), may or may not be digitally controlled, and therefore, may or may not ultimately be within the scope of the licensee's cyber security program. The licensee should conduct an initial consequence analysis of 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. This analysis should be conducted without accounting for existing mitigating measures to determine what the "worst case" impact would be if the CDA were to be compromised.

For those support systems or equipment not directly associated with SSEP functions, the licensee performs a dependency analysis to determine whether cyber compromise of those systems or equipment could adversely impact SSEP functions. If the analysis shows that such compromise, exploitation, or failure could adversely impact SSEP functions, then such systems themselves are considered CSs. The term "compromise" as used in the context of this guidance refers to a loss of confidentiality, integrity, or availability of data or system function.

The identification of CSs include those systems that (1) perform or are relied upon for SSEP functions, (2) affect SSEP functions or affect CSs and/or CDAs that perform SSEP functions, (3) provide a pathway to a CS and/or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS and/or CDA, or (5) protect any of the above from cyber attack up to and including the DBT. Figure 3 illustrates this evaluation process.

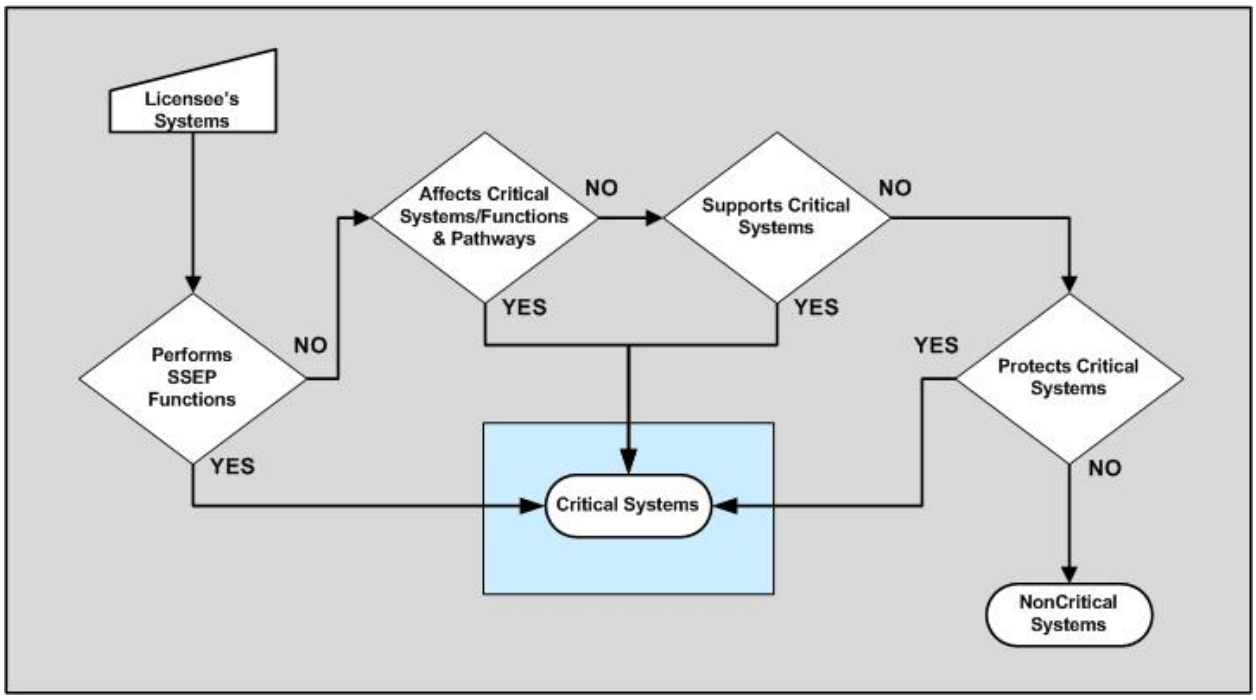

Figure 3 Evaluation process for determining critical systems

With the identification of the all the CSs the licensee should then analyze and identify which specific assets are actually CDAs, and thus within the scope of 10 CFR 73.54. A CDA may be a component of a CS, may protect a CS from cyber attack, or may be directly or indirectly connected to a CS. The direct connections may include a wired or wireless pathway (involving a chain of connections). The indirect connections may include "air-gapped" systems, CDAs behind a one-way security boundary device, or "sneaker nets" by which data or software is manually carried from one digital device to another and transferred using physically transportable storage medium, such as floppy disks, thumb drives, portable hard disks, or other modes of data transfer. Some helpful information sources for identifying CSs and CDAs include, but are not limited to, the final safety analysis report, the site-specific probabilistic risk assessment, technical specifications, and documents associated with the Maintenance Rule Program developed under 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants."

CDAs include those digital assets that (1) perform SSEP functions, (2) could adversely affect SSEP functions or CSs and/or CDAs that perform SSEP functions, (3) provide a pathway to a CS and/or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS and/or CDA, or (5) protect any of the above from cyber attack up to and including the DBT. Figure 4 illustrates the process of identifying CDAs.

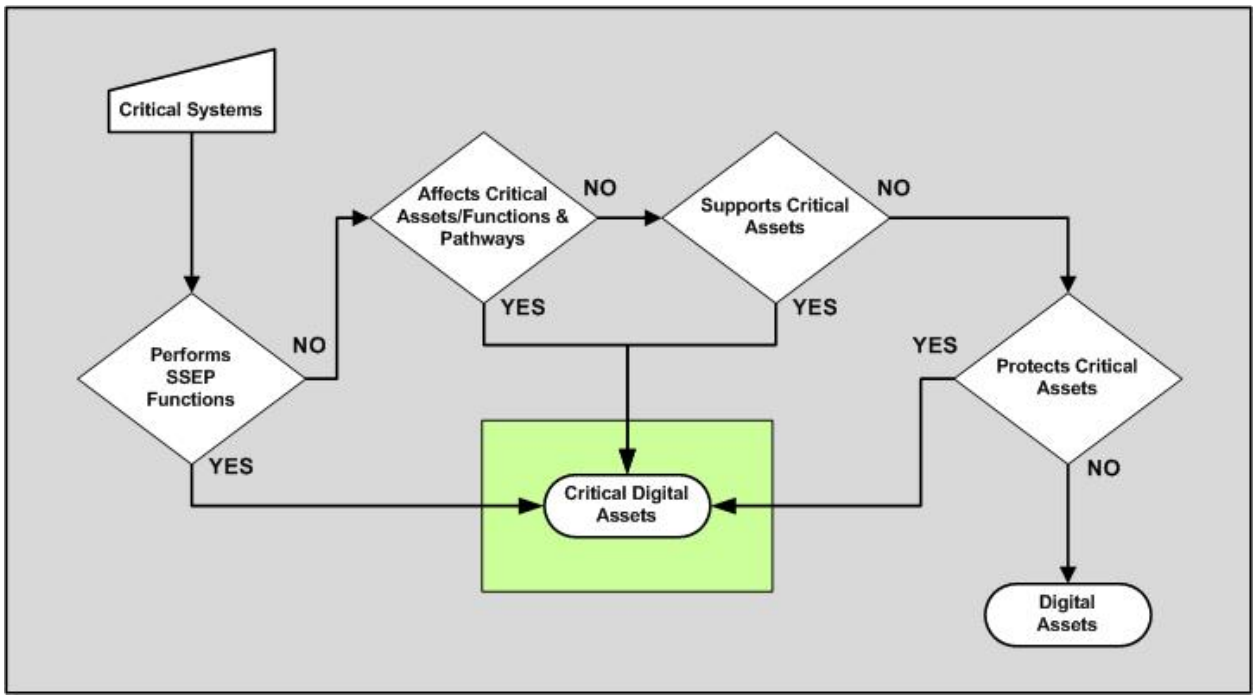

Figure 4 Evaluation process for identifying critical digital assets

Some CDAs and systems within a nuclear plant may be autonomous or standalone systems (i.e., they have no data connections to any other system). The lack of connectivity to other plant systems greatly enhances the cyber security posture for autonomous CDAs and systems or networks. This lack of connectivity reduces the possibility of compromise from cyber threats originating from sources external to the plant. However, such systems are still vulnerable to cyber attack originating from internal sources, such as inserting media into a system that has malicious code on it, diagnostic systems, and other offline connections and access. In addition, because of the abundance of off-the-shelf devices and peripherals that support communications technology, the architecture of an autonomous system is altered when such communication devices are intentionally or inadvertently introduced into the system. The regulations in 10 CFR 73.54 do not distinguish between autonomous and nonautonomous systems. Therefore, licensees should protect the security posture of an autonomous system with the same diligence they apply to interconnected systems.

To document the outcome of the identification process, the licensee should collect the following information:

- a general description of each system, asset, or network identified as a CDA and CS
- a brief description of the overall function provided by each CDA and CS
- an analysis that describes the potential consequence to both the CS and the SSEP functions if a compromise of the CDA or CS were to occur
- the function of the CDA (e.g., protection, control, monitoring, reporting, or communications),
- the identification of CDAs within each CS
- a description of the following security functional requirements and specifications:
  - developmental and evaluation-related assurance requirements

– information security requirements necessary for vendors or developers to maintain the integrity of acquired systems

Section 3.1.3 of Appendix A to this guide provides a template for licensees to use in preparing that section of the cyber security plan which discusses the identification of CDAs.

C.3.1.4 Review and Validation

The objectives of the review are to review and confirm the direct and indirect connectivity of each CDA, and identify pathways to CDAs. The licensee can then use this information in the next phases of its review to ensure that (1) CDAs are deployed in the correct layer of the security architecture described in Section C.3.2.1 of this guide (2) potential cyber security risks to CDA are addressed effectively as described in Section C.3.3 of this guide, and (3) the baseline configuration of each CDA is established for change control program. One acceptable method of conducting a review and validation includes the following activities:

- identify and document the physical and logical location of each CDA,
- identify and document direct and indirect connectivity pathways to and from the CDA,
- identify and document infrastructure interdependencies of the CDA, and
- identify and evaluate the effectiveness of any existing security controls (for existing plants) and the location of the CDA in the defensive architecture.

The licensee validates this information through a physical and electronic inspection of the system. The validation process includes the following activities:

- perform a physical inspection of the configuration of each CDA, including tracing all communication connections into and out of the CDA to each termination point along all communication pathways,
- examine the physical security established to protect each CDA and its communication pathways,
- examine and assess the configuration and effectiveness of security controls (e.g., firewalls, intrusion detection systems, data diodes) along the communication pathways,
- examine interdependencies with other CDAs and CSs and trust relationships between the CDAs and CSs,
- examine interdependencies with infrastructure support systems, emphasizing potential compromises of electrical power, environmental controls, and fire suppression equipment, and
- resolve information or configuration discrepancies identified during the reviews, including the presence of undocumented or missing connections, and other cyber security-related irregularities associated with the CDAs and CSs.

An electronic validation is an acceptable way for licensees to validate the review, if it is impractical to trace a communication pathway fully to its conclusion by means of a physical walkdown inspection. Electronic validation methods that provide equivalent to or better than connection validation compared to physical walkdowns is an acceptable method (e.g., a digital voltmeter, physical continuity validation). The walkdown should start with the CDA and work its way outward, inspecting connected hardware and interdependencies with critical support infrastructure (e.g., power; heating, ventilation, and air conditioning; fire suppression).

Section 3.1.4 of Appendix A to this document provides a template for licensees to use in preparing that section of the cyber security plan which addresses implementing the review and validation process.

C.3.2 Defense-in-Depth Protective Strategies

As stated in 10 CFR 73.54(c)(2), the licensee must design its cyber security program to apply and maintain integrate defense-in-depth protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks. To comply with this requirement, licensees implements an overall site defensive strategy consistent with the architecture described in Section C.3.2.1 of this guide, as well as the security controls identified in Section C.3.3 of this guide. Defense-in-depth strategies represent a documented collection of complementary and redundant security controls that establish multiple layers of protection to safeguard CDAs. Under a defense-in-depth strategy, the failure of a single protective strategy or security control should not result in the compromise of a safety, important-to-safety, security, or emergency preparedness function.

Defense-in-depth can be achieved in multiple ways. From a security architecture perspective, it involves setting up multiple security boundaries to protect CDAs and networks from cyber attack. In this way, multiple protection levels of mechanisms must fail for a cyber attack to progress and impact a CS or network. Therefore, defense-in-depth is achieved not only by implementing multiple security boundaries, but also by instituting and maintaining a robust program of security controls that assess, protect, respond, prevent, detect, and mitigates an attack on a CDA and with recovery.

For example, if a failure in prevention were to occur (e.g., a violation of policy) or if protection mechanisms were to be bypassed (e.g., by a new virus that is not yet identified as a cyber attack), mechanisms would still in place to detect and respond to an unauthorized alteration in an impacted CDA, mitigate the impacts of this alteration, and recover normal operations of the impacted CDA before an adverse impact.

C.3.2.1 Security Defensive Architecture

An overall cyber security defensive strategy for a site must employ defense-in-depth strategies to protect CDAs from cyber attacks up to and including the DBT. One acceptable method for achieving this goal is to incorporate a defensive architecture that establishes formal communication boundaries (or security levels) in which defensive measures are deployed to detect, prevent, delay, mitigate, and recover from cyber attacks. An example of such a defensive architecture is one that includes a series of concentric defensive levels of increasing security which conceptually correspond to existing physical security areas at a facility (e.g., vital area, protected area, owner-controlled area, corporate accessible area, public area).

Figure 5 provides an example of an acceptable cyber security defensive architecture. This defensive architecture includes five concentric cyber security defensive levels separated by security boundaries, such as firewalls and diodes, at which digital communications are monitored and restricted. Systems requiring the greatest degree of security are located within a greater number of boundaries. The logical model shown below does not always correspond directly with the physical locations such as the vital, protected or owner-controlled areas.

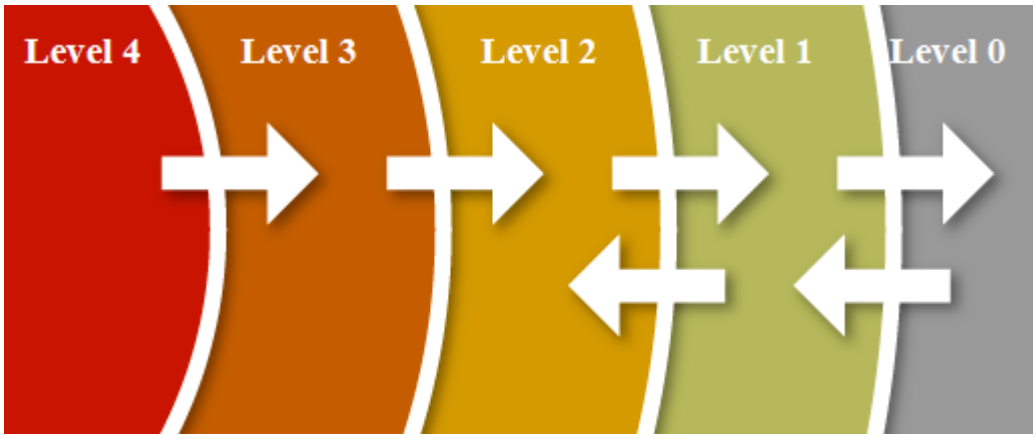

Figure 5 Simplified cyber security defensive architecture

An acceptable defensive architecture is one that includes the following characteristics:

- CDAs associated with safety, important to safety and security functions, as well as support systems and equipment which, if compromised, would adversely impact safety, important to safety and security functions, are allocated to Level 4 and are protected from all lower levels.
- Only one-way data flow is allowed from Level 4 to Level 3 and from Level 3 to Level 2.
- Initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited.
- Data only flows from one level to other levels through a device or devices that enforce security policy between each level.
- Maintains the capability to detect, prevent, delay, mitigate, and recover from cyber attacks.
- CDAs are configured as described in Section C.3.3 of this guide.
- Applications, services, and protocols not necessary to support the design-basis function of the contained CDAs are eliminated.
- CDAs and boundary protection systems are configured as described in Section 5 of Appendix B and Section 6 & 7 of Appendix C.

For this defensive architecture to be effective in protecting CDAs from cyber attacks the licensee consistently applies the above characteristics, along with the technical security controls discussed in Appendix B and the management and operational security controls discussed in Appendix C, and adopt the security controls identified in Section C.3.3 of this guide.

The NRC staff emphasizes that, while the defense model may allow communications between systems within the same level (e.g. Level 4 and/or Level 3), the digital isolation of CDAs (i.e., no communication pathways between a CDA and any other digital asset) is the most secure way to meet many of the requirements specified in 10 CFR 73.54. In particular, digital isolation is preferred whenever feasible.

Section 3.1.5 of Appendix A to this guide includes a template for licensees to use in preparing the section of the cyber security plan regarding implementation of defense-in-depth strategies.

C.3.3 Security Controls

As stated in 10 CFR 73.54(c)(1), the licensee must design its cyber security program to implement security controls to protect the CDAs from cyber attacks up to and including the DBT. A cyber compromise of CDAs would adversely impact nuclear facilities' SSEP functions that are necessary for protecting public health and safety. Because the SSEP functions are necessary in protecting the public health and safety, a cyber compromise of a CDA may cause high negative impact to the public health and safety. Thus to provide high assurance that CDAs are protected from cyber attacks, potential cyber risks of these CDAs must be addressed known potential cyber risks. One way to consistently address these known potential cyber security risks of a CDA is by developing cyber security controls by tailoring the "high impact" baseline security controls in NIST SP 800-53 and NIST SP 800-82 to the unique environments of a nuclear facility.

Sections C.3.3.1 (technical controls), C.3.3.2 (operational controls), and C.3.3.3 (management controls) of this guide provide an acceptable list of security controls to address potential cyber security risks. The NRC developed these controls by incorporating selected controls from NIST SP 800-53, NIST SP 800-82, and DHS ICS security guidance. These controls are consistent with the well-established and standardized method of performing a risk assessment to select the set of baseline security controls based on system categorization, as outlined in NIST SP 800-30 "Risk Management Guide for Information Technology Systems" and NIST SP 800-37, "Guide to Certification and Accreditation of Federal Information Systems," issued May 2004 (Ref. 14).

An acceptable method for applying security controls to the CDAs identified in Section C.3.1.3 to address potential cyber risks is to implement all of the security controls as described in Appendix C and, for each of the security controls identified in Appendix B, perform one or more of the following activities:

- Implement each of the security controls in Appendix B of this document.
- If a security control can not be implemented, alternative controls or countermeasures that eliminate threat/attack vectors associated with one or more of the security controls enumerated in Appendix B by:
  - documenting the basis for employing alternative countermeasures
  - performing and documenting the attack vector and attack tree analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater protection as the corresponding security control in Appendix B
  - implementing alternative countermeasures that provide at least the same degree of protection as the corresponding security control in Appendix B
- Conduct an attack vector and attack tree analyses of one or more specific security controls for a CDA to provide documented justification demonstrating that an attack vector does not exist (i.e., is not applicable), obviating the need for a specific security control.

A security control should not be applied if the control adversely impacts SSEP functions or performance (e.g., unacceptable change in system response time, undesirable increase in system complexity). When a security control is determined to have an adverse affect, alternate controls should be used by the licensee to protect the CDA from cyber attack up to and including the DBT consistent with the process described above. Any residual vulnerability in a CDA as a result of not implementing a security control for concern over its impact to CDA function or performance should be eliminated or mitigated by alternate controls.

Once the security controls have been implemented the CST performs both an effectiveness

analysis, as described in Section 4.1.2, and vulnerability assessments/scans of the CDAs, as described in Section 4.1.3, to verify that there is high assurance that CDAs are adequately protected from cyber attack, up to and including the DBT. If these effectiveness or vulnerability analyses identify a gap in the cyber security program, the licensee may need to implement additional security measures and controls not provided in Appendixes B and C.

Section 3.1.6 of Appendix A to this guide contains a template for licensees to use in preparing the section of the cyber security plan that describes the implementation of security controls.

C.3.3.1 Technical Controls

Technical controls are safeguards or protective measures that are executed through nonhuman mechanisms contained within the hardware, firmware, operating systems, or application software. The attributes within this class include access controls, audit and accountability, system and communications protection, and identification and authentication. With technical controls, actions are preplanned or preprogrammed and automatically execute in response to a triggering event or are configured to provide electronic enforcement of policy. These actions generally do not require human intervention. Sections C.3.3.1.1 through C.3.3.1.5 describe acceptable methods to implement technical security controls.

C.3.3.1.1 Access Control

Access control includes the following elements:

- a written policy that defines the purpose, scope, roles, responsibilities, and management commitments to provide high assurance that only authorized individuals, or processes acting on their behalf, access CDAs and perform authorized activities
- procedures to facilitate and maintain access control policy which describe the following:
  - 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)
  - system hardening (i.e., the identification and removal of unnecessary system services, communication pathways, data storage capabilities, and insecure communication protocols)
  - management of CDAs (i.e., establishing, activating, modifying, reviewing, disabling, and removing accounts)
  - auditing of CDAs (i.e., at least annually or immediately upon changes in personnel responsibilities or major changes in system configurations or functionality)
  - separation of duties (i.e., through assigned access authorizations)
- implementation of the security controls described in Section 1 of Appendix B to this guide.

C.3.3.1.2 Audit and Accountability

Audit and accountability includes the following elements:

- a written policy that defines the purpose, scope, roles, responsibilities, requirements, and management commitments to audit elements of a nuclear facility's cyber security program for effectiveness and to correct any finding to ensure that the cyber security program is effective in protecting SSEP functions,
- procedures to facilitate and maintain audit and accountability policy, and

- implementation of the security controls described in Section 2 of Appendix B to this guide.

C.3.3.1.3 System and Communications Protection

System and communications protection includes the following elements:

- a written policy that defines the purpose, scope, roles, and responsibilities necessary to mitigate the risk of unauthorized system or communications access that could result in a cyber attack that adversely impacts the SSEP functions of a nuclear facility,
- procedures to facilitate and maintain system and communications protection policy and associated system and communications protection controls, and
- implementation of the security controls described in Section 3 of Appendix B to this guide.

C.3.3.1.4 Identification and Authentication

Identification and authentication protection includes the following elements:

- management of user identifiers by the following methods:
  - uniquely identifying each user and application acting as a user
  - verifying the identity of each user and application acting as a user
  - receiving authorization to issue a user identifier from an appropriate organization official
  - ensuring that the user identifier is issued to the intended party
  - disabling user identifier after a predetermined defined time period of inactivity
  - archiving user identifiers
- management of CDA authenticators by the following methods:
  - 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
  - changing and refreshing authenticators periodically
- implementation of the security controls described in Section 4 of Appendix B to this guide.

C.3.3.1.5 System Hardening

System hardening for CDAs includes the following elements:

- a policy that defines the purpose, scope, roles, responsibilities, and management commitments to provide high assurance that all existing CDAs are securely configured to prevent unauthorized access and use
- procedures to facilitate and maintain system hardening policy
- implementation of the security controls described in Section 5 of Appendix B to this guide.

C.3.3.2 Operational Controls

Operational controls are protective measures typically performed by humans rather than by automated means. The attributes within this class include activities involving media protection, physical and environmental protection, personnel security, system and information integrity, contingency planning, incident response, maintenance, attack mitigation, continuity of functions, awareness and training, and

configuration management. Operational controls are documented in procedures to ensure accountability of actions by plant personnel and contractors. Sections C.3.3.2.1 through C.3.3.2.9 describe acceptable operational controls.

C.3.3.2.1 Media Protection

Media protection includes the following elements:

- a written policy that defines the purpose, scope, roles, responsibilities, and management commitments in the areas of media receipt, storage, handling, sanitization, removal, reuse, and disposal necessary to provide high assurance that the risk of unauthorized disclosure of information that could be used in a cyber attack to adversely impact the SSEP functions of the nuclear facility is prevented,
- procedures to facilitate and maintain the media protection policy, and
- implementation of the security controls described in Section 1 of Appendix C to this guide.

C.3.3.2.2 Personnel Security

Personnel security includes the following elements:

- a written policy that defines the scope of individuals covered and the roles, responsibilities, and accountability structure of the security program to provide high assurance that individuals who have unescorted access (electronic or physical) to CDAs are trustworthy and reliable,
- procedures to facilitate the implementation of the personnel security policy, and
- implementation of the security controls described in Section 2 of Appendix C to this guide.

C.3.3.2.3 System and Information Integrity

System and information integrity includes the following elements:

- a written policy that defines the purpose, scope, roles, and responsibilities to provide high assurance that information stored in CDAs is protected,
- procedures to facilitate and maintain the system and information integrity policy, and
- implementation of the security controls described in Section 3 of Appendix C to this guide.

C.3.3.2.4 Maintenance

Maintenance includes the following elements:

- a written policy that defines the purpose, scope, roles, responsibilities, and management commitments associated with performing routine and preventative maintenance on CDAs and security boundary devices necessary to provide high assurance that the SSEP functions of the nuclear facility are protected from cyber attacks,
- procedures to facilitate and maintain the maintenance policy, and
- implementation of the security controls described in Section 4 of Appendix C to this guide.

C.3.3.2.5 Physical and Environmental Protection

Physical and environmental protection includes the following elements:

- a written policy that defines the purpose, scope, roles, responsibilities, and management commitments to provide a degree of high assurance of the following:
  - mitigation of the risk of unauthorized physical access to CDAs and associated communication pathways
  - protection of CDAs and associated communication pathways from environmental conditions that could cause the failure or improper functioning of infrastructure support systems (e.g., power supplies; heating, ventilation, and air conditioning systems; and fire suppression systems)
- procedures to facilitate and maintain physical and operational environment protection policy
- implementation of the security controls described in Section 5 of Appendix C to this guide.

C.3.3.2.6 Incident Response

Consistent with the requirements stated in 10 CFR 73.54(c)(3) and 10 CFR 73.54(c)(4), licensees must design their cyber security program to mitigate the adverse effects of cyber attacks and ensure that the functions of protected assets identified in 10 CFR 73.54(a)(1) are maintained. In addition, consistent with the requirements stated in 10 CFR 73.54(e)(2), the cyber security plan (and therefore the cyber security program) must include incident response and recovery measures by describing how to:

- maintain the capability for timely detection and response to cyber attacks,
- mitigate the consequences of cyber attacks,
- correct exploited vulnerabilities, and
- restore affected systems, networks, and equipment affected by cyber attacks.

An acceptable method for licensees to comply with these response and recovery requirements during and after a cyber attack is to include the following elements:

- develop an incident response policy that defines the purpose, scope, roles, responsibilities, and management commitments to plan and respond to a cyber security incident in a manner that provides high assurance that the consequences of a cyber attack can be mitigated to an acceptable level.
- develop procedures to facilitate the implementation of incident response policy and associated incident response measures.
- develop procedures to facilitate the implementation of the incident response investigations based on the guidance found in the following:
  - NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," August, 2006 (Ref. 15),
  - U.S. Department of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," 2004 (Ref. 16), and
  - U.S. Department of Justice, "Electronic Crime Scene Investigation: A Guide for First Responders," Second Edition, 2008 (Ref. 17).
- implement the security controls described in Section 8 of Appendix C to this guide.

The licensee should integrate incident response and recovery measures into the cyber security program and the emergency preparedness plan.

C.3.3.2.7 Contingency Planning/Continuity of SSEP Functions

As required by 10 CFR 73.54(c)(4), the licensee must design its cyber security program to ensure that cyber attacks do not adversely affect the functions of protected assets identified in 10 CFR 73.54(a)(1). An acceptable method for licensees to comply with the contingency planning requirements is to include the following elements:

- develop and implement a continuity of operation policy that defines the purpose, scope, roles, responsibilities, and management commitments to properly plan and initiate a cyber security incident recovery plan to provide high assurance that continuity of operations of the SSEP functions is maintained following a cyber attack.
- develop and implement procedures to facilitate and maintain the continuity of operations policy.
- implement the security controls described in Section 9 of Appendix C to this guide.

C.3.3.2.8 Awareness and Training

As required by 10 CFR 73.54(d)(1), the licensee must ensure, as part of its cyber security program, that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities effectively. An acceptable method for licensees to comply with the awareness and training requirements is to include the following elements:

- develop, disseminate, and periodically review and update a cyber security training and awareness plan that defines the purpose, scope, roles, responsibilities, and management commitment to provide high assurance that individuals have received training to properly perform their job functions.
- perform gap analysis in areas where additional training is needed.
- Establish measures to determine whether policies and procedures are being followed, and if not, whether a training or awareness issue is the cause and for measures to be taken to correct the deficiency.
- develop, disseminate, and periodically review and update procedures to facilitate and maintain the security training and awareness program.
- implement the security controls described in Section 10 of Appendix C to this guide.

C.3.3.2.9 Configuration Management

As stated in 10 CFR 73.54(d)(3), the licensee, as part of its cyber security program, must evaluate modifications to assets identified by 10 CFR 73.54(a)(1) before their implementation to ensure that the cyber security performance objectives identified in 10 CFR 73.54(a)(1) are maintained. An acceptable method for licensees to comply with the configuration management requirements is to include the following elements:

- develop, disseminate, and annually review and update the configuration management policy and program which defines the purpose of the nuclear facility's configuration management policy, scope, roles, requirements, responsibilities, and management commitments necessary to provide, with high assurance, that (1) when a modification to a CDA does not reduce the existing security and (2) any unauthorized or inadvertent modification of a CDA is prevented. The configuration management policy and program must apply to both licensee and vendor personnel.

- develop procedures to facilitate and maintain the configuration management policy and program and associated configuration management controls and measures.
- implement the security controls described in Section 11 of Appendix C to this guide.

C.3.3.3 Management Controls

Management controls are those that concentrate on the management of risk and the security policy environment. The attributes within this class cover activities involving system or service acquisitions, security assessments and risk management, and the addition and modification of digital assets. Sections 3.3.3.1 and 3.3.3.2 describe acceptable management controls.

C.3.3.3.1 System and Service Acquisition

An acceptable approach to system and service acquisition includes all of the following:

- development of a procurement policy that defines the purpose, scope, roles, responsibilities, and management commitments to provide high assurance that the integrity of systems and services is maintained during the procurement process,
- development of procedures to facilitate and maintain the implementation of procurement policies associated with vendor security and development life cycles, and
- implementation of the security controls described in Section 12 of Appendix C to this guide.

For safety systems, this section provides additional guidance when applying regulatory positions Section 2.1 through Section 2.6 of RG 1.152, Rev 2 (Ref 10).

C.3.3.3.2 Security Assessment and Risk Management

Consistent with the requirements of 10 CFR 73.54(d)(2), a licensee's cyber security program must ensure that cyber security risks are appropriately managed and evaluated. An acceptable method to comply with this regulation is to establish a risk management and evaluation program that performs the steps specified in Section 3.2 of this guide, Section 4 of Appendix A to this guide, and Section 13 of Appendix C to this guide to achieve a high degree of assurance that installed CDAs are protected against cyber attacks.

C.3.4 Incorporating the Cyber Security Program into the Physical Protection Program

Consistent with the requirements of 10 CFR 73.54(b)(3), a licensee must incorporate the cyber security program into its physical protection program. The physical protection program, as required by 10 CFR 73.55, provides organizational objectives and requirements that describe the protection measures necessary for a comprehensive approach to a licensee's overall security posture. While the methods and tools employed in the conduct of a cyber security attack may differ from that of a physical attack, the resulting effects can be similar. Furthermore, a cyber attack may be coordinated with a physical attack or may be used to assist a physical attack. As such, a licensee's physical protection program must be designed to protect the facility from physical, cyber, and combined attacks up to and including the DBT.

An acceptable method for complying with this requirement is to consider cyber attacks during the development and identification of target sets required by the physical security program and 10 CFR 73.55(f)(2) and to integrate the management of physical and cyber security. Some elements of this integration should consider the following:

- forming a unified security organization, which incorporates both cyber and physical security, that is independent from operations,
- analyzing, identifying, and documenting physical security and cyber security interdependencies,
- developing policies and procedures to integrate and unify management of these interdependencies,
- incorporating and unifying policies and procedures to follow consistent approaches to securing the plant from attacks up to and including the DBT,
- coordinating acquisition of physical or cyber security devices and equipment,
- coordinating interdependent physical and cyber security activities and training with physical and cyber security personnel,
- integrating and coordinating incident response capabilities with physical and cyber incident response personnel,
- training senior management regarding the needs of both disciplines, and
- periodically exercising the entire security force using multiple realistic scenarios combining both physical and cyber simulated attacks.

Section 3.2 of Appendix A to this guide contains a template for licensees to use in preparing the section of the cyber security plan that describes the process for integrating the cyber security program into the physical security program.

C.3.5 Policies and Implementing Procedures

As required by 10 CFR 73.54(f), the licensee must develop and maintain site-specific written policies and procedures to implement the cyber security program. The licensee need not submit these policies, implementing procedures, site-specific analyses, or other supporting technical information of the cyber security plan to the NRC for prior review and approval, but such information must be available for inspection by the NRC staff. The licensee must develop and implement a cyber security program that includes policies and procedures that describe the overall security goals, objectives, practices, and roles and responsibilities within the licensee's organization and, with high assurance, confirm that the cyber security program at a nuclear facility is properly established and maintained so as to protect the SSEP functions of the nuclear facility from cyber attacks. Section 3.1.2 of this guide describes a method that licensees can use to develop roles and responsibilities.

An acceptable method for licensees to comply with the policies and implementing procedures requirements is to perform the following:

- routinely review site policies and procedures to provide high assurance that they continue to adequately address the risks to the CDAs that they are intended to protect.
- evaluate issues related to technology evolution.
- address risks associated with employee positions.
- implement the policies and procedures described in the security controls in Appendices B and C to this guide.

C.4 Maintaining the Cyber Security Program

Once the security program is in place, 10 CFR 73.54(d)(2) states that licenses shall "evaluate and manage cyber risk." One acceptable method of doing so is to establish a security life cycle for CDAs that includes the following elements:

- continuous monitoring and assessment,
- configuration management,
- change management,
- security impact analysis of changes and environment,
- effectiveness analysis,
- ongoing assessment of security controls and programs effectiveness,
- vulnerability scans/assessments,
- change control, and
- security program review.

Sections C.4.1 through C.4.3 describe these elements.

C.4.1 Continuous Monitoring and Assessment

Continuous monitoring and assessment ensures that the periodic review and testing of security controls, processes, and procedures are conducted to confirm that the established security controls remain in place and that change(s) in the system, network, environment or emerging threats do not diminish their effectiveness.

Continuous monitoring includes the following:

- ongoing assessments of verify that the security controls implemented for each CDA remain in place throughout the life cycle,
- verification that rogue assets are not connected to the infrastructure,
- ongoing assessments of the need for and effectiveness of the security controls identified in Appendices B and C to this guide, and
- periodic cyber security program reviews to evaluate and improve the effectiveness of security program.

Continuous monitoring may require updates to the cyber security plan to reflect changes necessary to maintain high assurance that CDAs are adequately protected from cyber attacks. Section 4.1 of Appendix A to this guide provides a template for licensees to use in preparing of the cyber security plan regarding implementation of the continuous monitoring process for security controls.

C.4.1.1 Ongoing Assessments of Security Controls

Ongoing assessments of security controls ensure that implemented security controls remain in place and function correctly. Licensees should verify the status of these security controls on an annual basis at a minimum or more frequently, depending on the specific requirements for each security control, as described in Appendices B and C to this guide. Section 4.1.1 of Appendix A to this guide contains a template for licensees to use in preparing the cyber security plan regarding implementation of the ongoing assessment process for security controls.

C.4.1.2 Effectiveness Analysis of Security Controls

Experience has shown that adversaries continually gain additional capabilities, while new vulnerabilities and flaws are discovered. An effectiveness analysis evaluates the continuing adequacy of

established security controls in an environment of ever-changing cyber security threats and vulnerabilities. The licensee should verify the effectiveness of security controls on at least an annual basis or more frequently, depending on the specific requirements for each security control, as described in Appendices B and C.

Reviews of the security program and controls should include, but not be limited to, periodic audits of the physical security program, security plans, security controls, implementing procedures, and cyber security programs; safety/security interface activities; re-evaluating assumptions and conclusions about current cyber security threats; the testing, maintenance, and calibration program; and feedback from external entities. These reviews should encompass components that undergo scheduled maintenance and include information regarding the efficiency of the periodic maintenance and life cycle support activities.

Effectiveness and efficiency measures two aspects of security control implementation:

(1) the robustness of the security control, referred to as effectiveness, and
(2) the timeliness of the result, that the control is designed to produce, referred to as efficiency.

Based on this information, a gap analysis should be performed to identify areas of improvement. The effectiveness evaluation also provides key information about the results of previous policy and acquisition decisions. These measurements:

- provide insight for improving performance of the cyber security program,
- assist in ascertaining whether specific security controls are functioning properly and 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 directly tied to security control implementation.

Section 4.1.2 of Appendix A to this guide includes a template for the licensee to use in preparing the cyber security plan regarding implementation of the effectiveness analysis of security controls.

C.4.1.3 Vulnerability Scans and Assessments

Vulnerability scans and assessments identify security deficiencies in CDAs. Licensees should conduct periodic vulnerability scanning of all CDAs at least [quarterly], when specified by the security controls described in Appendices B and C to this guide, and when new vulnerabilities that could potentially affect the security posture of CDAs are identified.

Licensees should employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process. Licensees should analyze vulnerability scan reports and address those vulnerabilities that pose a risk to CDAs and SSEP functions at the site. In addition, licensees should ensure that similar vulnerabilities which may impact interconnected or other CDAs are understood, evaluated, and mitigated.

Licensees should ensure that the scanning process does not adversely impact SSEP functions. If this could occur, licensees should remove CDAs from service (or replicate) before scanning is conducted. Section 4.1.3 of Appendix A to this guide includes a template for licensees to use in preparing the cyber security plan regarding implementation of the vulnerability scans and assessments of security controls.

C.4.2 Change Control

Change control ensures that additions to or modifications of CDAs (or changes to their environment) are introduced in a controlled and coordinated manner. To prepare a change control program the licensees (1) implement Section 4.2 of Appendix A and the security controls in Section 11 of Appendix C and then (2) establish, maintain, and document a baseline configuration of the CDAs. This baseline includes, at a minimum, a current list of all components (e.g., hardware, software), configuration of peripherals and software, version releases of current software, and switch settings of machine/hardware components.

The documentation necessary for effective change management includes, but is not limited to, a log of configuration changes which identifies the personnel who authorized and implemented the changes, the date and time of the changes, the purpose of the change, validation of the effectiveness of the security controls, and any observations made during the course of the change. Appendices A and C to this guide provide additional guidance on change control.

C.4.2.1 Configuration Management

Configuration management ensures that the site's cyber security program objectives remain satisfied by controlling the changes made to CDAs throughout their life cycle. During the operation and maintenance phases of the CDA life cycle, effective configuration management ensures that changes made to CDAs are conducted using processes and procedures that will not introduce additional security risks into the system. Configuration management also ensures that licensees implement each of the controls specified in Appendices B and C to this guide in a timely and effective manner. Change control is an essential element of managing cyber security by minimizing the possibility that unanalyzed components will be introduced within the CDAs, or facility.

Licensees should evaluate modifications to CDAs before their implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained. Section 4.2.1 of Appendix A to this guide includes a template for licensees to implement configuration management by (1) following the process described in Section 4.2.1 and (2) creating CDA security and configuration management documentation for all CDAs when such documentation is either unavailable or nonexistent (e.g., due to the age of the digital asset, lack of support from the vendor or contractor). This formal documentation should include the basis for not implementing one or more of the technical security controls specified in Appendix B to this guide.

C.4.2.2 Security Impact Analysis

The security impact analysis assists in managing potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats. Section 4.2.2 of Appendix A to this guide includes a template for licensees to perform a security impact analysis before making a design or configuration change to a CDA or when changes to the environment occur.

Licensees should evaluate, document, and incorporate into the security impact analysis safety and security interdependencies of other CDAs or systems, as well as the following:

- updates to the location of the CDA and connected assets;
- updates to connectivity pathways (direct and indirect);
- updates to infrastructure interdependencies;

- updates to the application of defensive strategies, including defensive architectures, security controls, and other defensive strategy measures;
- updates to the documentation of plantwide physical and cyber security policies and procedures, including attack mitigation and incident response and recovery; and
- updates to procedures for screening, evaluating, mitigating, and dispositioning threat and vulnerability notifications received from credible sources.

Licensees should perform these impact analyses as part of the configuration management process to assess the impacts of the changes on the security posture of CDAs that can affect site SSEP functions. At the completion of the analysis the licensees implements new security controls, as described in Section 4.2.2, to mitigate any gaps identified in the analysis.

Section 4.2.2 of Appendix A to this guide includes a template for licensees to use in preparing the cyber security plan regarding security impact analysis.

C.4.3 Cyber Security Program Review

In accordance with 10 CFR 73.54(g), the licensee must review the cyber security program as a component of the physical security program, consistent with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The final major element of maintaining an effective cyber security program is to conduct periodic security program reviews. The cyber security program establishes the necessary measures and governing procedures to implement reviews of applicable program elements, in accordance with the requirements of 10 CFR 73.55(m). The periodic security program review serves to evaluate the overall effectiveness of the cyber security program. An acceptable approach to cyber security program review includes the following:

- develop and implement a review program that addresses the purpose, scope, roles, responsibilities, requirements, and management commitments associated with reviewing the elements of the security program for effectiveness.
- develop and implement procedures to facilitate and maintain the review program.

Licensees should complete a program review at least every 24 months. In addition, licensees should conduct reviews:

- within 12 months after initial implementation of the program,

- whenever a change is made to the operating environment that could have an adverse impact on security,

- as necessary based upon site-specific analyses, assessments, or other performance indicators using individuals independent of those personnel responsible for program management or implementation.

As per 73.55(m)(3) licensees must document the results and recommendations of the program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews in a report, which should be reviewed by an individual at least one level higher than those having responsibility for day-to-day plant operation. Licensees must maintain these reports in an auditable form and make them available to inspectors upon request.

Section 4.3 of Appendix A to this guide includes a template for licensees to use in documenting this process in a cyber security plan.

C.5 Records Retention and Handling

In accordance with 10 CFR 73.54(h), the licensee must retain all records and supporting technical documentation required to satisfy the requirements of this regulation until the Commission terminates the license for which the records were developed. Furthermore, the licensee must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

An acceptable method for complying with this requirement is for the licensee to maintain records or supporting technical documentation so that inspectors, auditors, or assessors will have the ability to evaluate incidents, events, and other activities that are related to any of the cyber security elements described, referenced, and contained within the licensee's NRC-approved cyber security plan. Records required for retention include, but are not limited to, digital records, log files, audit files, and nondigital records that capture, record, and analyze network and CDA events. Licensees should retain these records to document access history and discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions. Section 5 of Appendix A to this guide includes a template for the licensee to use in preparing the cyber security plan regarding records retention and handling of security controls.

D IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC's plans for using this regulatory guide. This regulatory guide provides applicants and licensees with new guidance on methods that the NRC staff considers acceptable for the protection of digital computer and communication systems and networks, as set forth in 10 CFR 73.54, 10 CFR 73.55, and 10 CFR 50.34. The NRC prepared a backfit analysis for the proposed regulations at 10 CFR 73.55, from which the requirements of 10 CFR 73.54 have been derived. The NRC has determined that, in accordance with 10 CFR 50.109(a)(3), a substantial increase in the overall protection of the public health and safety or the common defense and security will be derived from the backfit associated with 10 CFR 73.54, and the direct and indirect costs of implementation are justified in view of this increased protection.

In some cases, applicants or licensees may propose or use a previously established acceptable alternative method for complying with specified portions of the NRC's regulations. Otherwise, the methods described in this guide will be used in evaluating compliance with the applicable regulations for license applications, license amendment applications, and amendment requests.

GLOSSARY

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

adversary— individual, group or organization that conducts or has the intent to conduct detrimental activities.

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

automated—An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Used in both the singular and plural cases (Source: NIST).

authentication—Verifying the identity of a user and application acting as a user or verifying the origin of a data, messages, or commands. Authentication depends on four classes of data, generally summarized as "what you know," "what you have," "what you are," and "what you do."

bidirectional communications—Transmission and receipt of data or signals between devices occurring in either direction along a communications medium. TCP is an example of bidirectional communications protocol.

boundary—A point of demarcation that physically and logically separates defensive levels having different security requirements.

boundary interface—A boundary across which communication occurs between critical digital assets, systems, or networks contained within adjacent defensive levels.

commercial off-the-shelf —Software or hardware products that are ready made and available for sale to the general public.

contingency plan—Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster (Source: NIST SP 800-34).

credible—Information received from a source determined to be reliable (e.g., law enforcement, Government agency, US CERT) or has been verified to be true. A threat or vulnerability can be verified to be true or considered credible when (1) evidence supporting the threat or vulnerability exists, (2) information independent from the actual threat message or vulnerability exists that supports the threat or vulnerability, or (3) a specific known group or organization claims responsibility for the threat or vulnerability.

countermeasure— action, measure, or device that reduces risk.

critical digital asset (CDA)—A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network.

critical system (CS)—An analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function.

custodian—One who guards and protects or maintains, especially one entrusted with guarding and maintaining property or records.

cyber attack—The manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may (1) originate from either inside or outside the licensee's facility, (2) have internal and external components, (3) involve physical or logical threats, (4) be directed or non directed in nature, (5) be conducted by threat agents having either malicious or non malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to critical digital assets or critical systems. This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information, the attempt to compromise a CDA and/or CSs integrity, availability, or confidentiality or the attempt to cause an adverse impact to a SSEP function. Further background on cyber attacks which are up to and including DBT, can be found in Sections 1.1(c), 1.2, and 1.5 of Regulatory Guide 5.69, and the cyber attack may occur individually or in any combination.

defense-in-depth—An approach to security in which multiple levels of security and methods are deployed to guard against failure of one component or levels.

Host-based Intrusion Detection System (HIDS)—An application that detects possible malicious activity on a host from characteristics such as change of files (file system integrity checker), operating system call profiles, etc.

incident—Occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action.

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

Intrusion Detection System (IDS)—A system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include intrusions, misuse, unauthorized access or malicious or abnormal operation. These systems may be network or host based. Intrusion detection functions include monitoring and analyzing both user and system activities, analyzing system configurations and vulnerabilities, assessing system and file integrity, recognizing patterns typical of attacks, analyzing abnormal activity patterns, and tracking user policy violations.

Intrusion Prevention System (IPS)—An intrusion detection system that has the ability to take actions to pre-empt or stop activities identified as malicious.

malware—Malicious software designed to infiltrate or damage a CDA, without the Licensee/Applicants consent. Malware is taken to include computer viruses, worms, Trojan horses, Root kits, spyware and adware.

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

network—group of components that share information or interact with each other in order to perform a function.

patch—A fix for a CDA or software program where the actual binary executable and related files are modified.

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

remote access—The ability to access a critical digital asset, computer, node, or network resource located within an identified defensive level from a critical digital asset, computer, or node that is physically located in a less secure defensive level.

sanitization— Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

security monitoring network—A physically separate network that is provided to support the cyber security infrastructure with an equal or greater security level than the security levels it is supporting.

support equipment—Equipment that directly or indirectly supports the operation or functionality of systems associated with safety, important to safety, security or emergency preparedness functions and if compromised, the equipment could adversely impact safety, important to safety, security or emergency preparedness functions. Examples of support equipment include, but are not limited to, handling, testing and maintenance equipment and parts, which if compromised could have an adverse impact on the safety, important to safety, security or emergency preparedness functions.

support system—A system that directly or indirectly supports the operation or functionality of systems associated with safety, important to safety, security or emergency preparedness functions and if compromised, the system could adversely impact safety, important to safety, security or emergency preparedness functions. Examples of support systems include, but are not limited to, electrical power, heating, ventilation, and air conditioning, communications, fire suppression, or any system, which if compromised could have an adverse impact on the safety, important to safety, security or emergency preparedness functions.

threat—natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.

vulnerability—feature, attribute or weakness in a system's design, implementation, or operation and management that could render a CDA open to exploitation or SSEP function susceptible to adverse impact.

REFERENCES[1]

1. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

2. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

3. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.

4. NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC, February 2002.

5. NRC Order EA-03-086, "Design Basis Threat for Radiological Sabotage," U.S. Nuclear Regulatory Commission, Washington, DC, April 2003.

6. NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," October 2004.

7. Zimmerman, R. P., Letter to Coyle, M.T., NEI, Subject: "NRC Acceptance of NEI 04-04, "Cyber Security Program for Power Reactors," Revision 1," December 23, 2005.

8. NEI 04-04, Rev. 1, "Cyber Security Program for Power Reactors," Nuclear Energy Institute, November 18, 2005.[2]

9. NIST SP 800-53, Rev. 3, "Recommended Security Controls for Federal Information Systems," National Institute of Standards and Technology, Gaithersburg, MD, August 2009.

10. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission.

11. IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Washington, DC, September 11, 2003.

12. Branch Technical Position 7-14, Rev. 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Washington, DC, March 2007.

---

[1] Publicly available NRC published documents such as Regulations, Regulatory Guides, NUREGs, and Generic Letters listed herein are available electronically through the Electronic Reading room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail PDR.Resource@nrc gov.

[2] Copies of the non-NRC documents included in these references may be obtained from the publishing organization.

13. NIST SP 800-82, "Guide to Industrial Control Systems Security," National Institute of Standards and Technology, Gaithersburg, MD, September 29, 2008.

14. NIST SP 800-37, "Guide to Certification and Accreditation of Federal Information Systems," National Institute of Standards and Technology, Gaithersburg, MD, May 2004.

15. NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology, Gaithersburg, MD, August 2006.

16. U.S. Department of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," 2004.

17. U.S. Department of Justice, "Electronic Crime Scene Investigation: A Guide for First Responders," Second Edition, 2008.

BIBLIOGRAPHY

American National Standards Institute (ANSI)

ANSI ISO/IEC 17799, "Information Technology Security Techniques: Code of Practice for Information Security Management," 2005.

ANSI ISO/IEC TR 13335-1, "Information Technology: Guidelines for the Management of IT Security—Part 1: Concepts and Models," 1996.

ANSI ISO/IEC TR 13335-3, "Information Technology: Guidelines for the Management of IT Security—Part 3: Techniques for the Management of IT Security," 1998.

ANSI ISO/IEC TR 13335-4, "Information Technology: Guidelines for the Management of IT Security—Part 4: Selection of Safeguards," 2000.

ANSI ISO/IEC TR 13335-5, "Information Technology: Guidelines for the Management of IT Security—Part 5: Management Guidance on Network Security," 2001.

National Institute of Standards and Technology (NIST)

NIST SP-50, "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology, Gaithersburg, MD.

NIST SP 800-64, Rev. 2, "Security Considerations in the System Development Life Cycle," National Institute of Standards and Technology, Gaithersburg, MD, October 2008.

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.

APPENDIX B

TECHNICAL SECURITY CONTROLS

B.1 Access Controls

B.1.1 Access Control Policy and Procedures

[Licensee/Applicant] developed, disseminated, and [annually] reviews and updates a formal, documented, "critical digital asset" (CDA) access control policy which addresses the purpose, scope, roles, responsibilities, management commitments, and internal coordination of such policy. [Licensee/Applicant] has also developed formal, documented procedures to 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, 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 functions, least privilege, unsuccessful login attempts, system use notification, previous login notification, session lock, supervision and review/access control, permitted actions without identification or authentication, automated marking, automated labeling, network access control, open/insecure protocol restrictions, wireless access restrictions, insecure and rogue connections and access control for portable and mobile devices and use of external CDAs proprietary protocol visibility, third party products and controls, and use of external systems.

The access control policy addresses the following:

- 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., establishing, activating, modifying, reviewing, disabling, and removing accounts),
- protection of password/key databases to prevent unauthorized access to master user and password lists,
- auditing of CDAs [annually] or immediately upon changes in personnel responsibilities or major changes in system configurations or functionality, and
- separation of duties (i.e., through assigned access authorizations).

B.1.2 Account Management

[Licensee/Applicant] is responsible for the following:

- managing and documenting CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts,
- reviewing CDA accounts in a manner consistent with the access control list provided in the [design control package, access control program, cyber security procedures] and initiating required actions on CDA accounts [no less frequently than once every 30 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,

- reviewing and documenting CDA accounts at a maximum interval consistent with the most recent version of Nuclear Energy Institute (NEI) 03-12, "Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan," endorsed by the U.S. Nuclear Regulatory Commission (NRC), and
- employing automated mechanisms that support CDA account management functions and enable CDA to automatically:
  - terminate temporary, guest, and emergency accounts [no less frequently than once every 30 days]
  - disable inactive accounts [no less frequently than once every 30 days]
  - create and protect audit records for account creation, deletion, and modification
  - document and notify system administrators of all account creation, deletion, and modification activities so that system administrators are aware of any account modifications and can investigate potential cyber attacks in a timely manner.

B.1.3 Access Enforcement

[Licensee/Applicant] is responsible for the following:

- enforcing assigned authorizations for controlling access to CDAs in accordance with established policies and procedures,
- assigning all user rights and privileges on the CDA consistent with the user authorizations,
- defining and documenting privileged functions and security-relevant information for the CDAs,
- authorizing personnel access to privileged functions and security-relevant information consistent with established policies and procedures,
- restricting access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to authorized personnel (e.g., security administrators),
- defining and documenting privileged functions for CDAs,
- requiring dual authorization for critical privileged functions and the creation of any privileged access for users, and
- ensuring and documenting that access enforcement mechanisms do not adversely impact the operational performance of CDAs and employing alternate compensating security controls when access enforcement cannot be used.

B.1.4 Information Flow Enforcement

[Licensee/Applicant] is responsible for the following:

- enforcing and documenting 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,
- maintaining documentation that demonstrates that [Licensee/Applicant] has analyzed and addressed the types 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,
- implementing and documenting information flow control enforcement using protected processing level (e.g., domain type-enforcement) as a basis for flow control decisions,
- implementing near-real time capabilities to detect, deter, prevent, and respond to illegal or unauthorized information flows,
- preventing encrypted data from bypassing content-checking mechanisms,
- implementing 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, and
- configuring CDAs such that user credentials are not transmitted in clear text and documenting this requirement in the access control policy.

B.1.5 Separation of Functions

[Licensee/Applicant] is responsible for the following:

- establishing and documenting divisions of responsibility and separating functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals,
- enforcing separation of CDA functions through assigned access authorizations,
- implementing alternative controls and documenting the justification for alternative controls and countermeasures for increased auditing for those situations in which a CDA cannot support the differentiation of roles and a single individual must perform all roles within the CDA, and
- restricts security functions to the least amount of users necessary to ensure the security of CDAs.

B.1.6 Least Privilege

[Licensee/Applicant] is responsible for the following:

- assigning the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks,
- configuring CDAs to enforce the most restrictive set of rights and privileges or access needed by users, and
- implementing alternative controls and documenting the justification for alternative controls and countermeasures for increased auditing for situations in which a CDA cannot support the differentiation of privileges within the CDA and an individual must perform all roles within the CDA.

B.1.7 Unsuccessful Login Attempts

[Licensee/Applicant] ensures the following:

- Security controls are implemented to limit the number of invalid access attempts by a user. The access control policy documents this requirement. The number of failed login attempts in a specified time period may vary by CDA. For example, more than three invalid attempts within a 1-hour time period will automatically lock out the account. The [Licensee/Applicant] system enforces the lock out mode automatically.
- The access control policy includes a requirement that only authorized individuals, who are not the user, can unlock accounts once the maximum number of unsuccessful login attempts has been exceeded. Alternatively, other verification techniques or mechanisms that incorporate identity challenges are used.
- The access control policy documents the justification and details for alternative controls or countermeasures for those instances in which a CDA cannot support account/node locking or delayed login attempts. If a CDA cannot perform account/node locking or delayed logins because of significant adverse impact on performance, safety, or reliability, the [Licensee/Applicant] employs alternative controls or countermeasures that include the following:
  - real-time logging and recording of unsuccessful login attempts, and

- 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.

B.1.8 System Use Notification

[Licensee/Applicant] ensures the following:

- A "system use notification" message is displayed before granting system access informing potential users of the following:
  - The user is accessing a restricted system.
  - System usage is monitored, recorded, and subject to audit.
  - Unauthorized use of CDA is prohibited and subject to criminal and civil penalties. The use of CDAs indicates consent to monitoring and recording.
- The CDA system use notification message provides privacy and security notices.
- The CDA system use notification message is approved before its use.
- The CDA system use notification message remains on the screen until the user takes explicit actions to log on to the CDA.
- Physical notices are installed in those instances in which a CDA cannot support system use notifications.

B.1.9 Previous Logon Notification

[Licensee/Applicant] is responsible for the following:

- upon successful logon, configuring CDA to display the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon, and
- requiring all end users to report any suspicious activity to the Cyber Security Program manager.

B.1.10 Session Lock

[Licensee/Applicant] configures CDAs to do the following:

- initiate a session lock after [within 30 minutes of inactivity],
- provide the capability for users to directly initiate session lock mechanisms,
- maintain the session lock on a CDA until the user reestablishes access using identification and authentication procedures, and
- implement alternative controls and document the justification for alternative controls or countermeasures for those instances in which a CDA cannot support session locks and:
  - physically restrict access to the CDA,
  - monitor and record physical access to the CDA to detect and respond to intrusions in a timely manner,
  - use auditing or validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - ensure that individuals who have access to the CDA are qualified, and
  - ensure that those individuals are trustworthy and reliable, in accordance with 10 CFR 73.56.

B.1.11 Supervision and Review—Access Control

[Licensee/Applicant] is responsible for the following:

- documenting, supervising, and reviewing the activities of users with respect to the enforcement and usage of access controls, and
- employing automated mechanisms within CDAs to support and facilitate the review of user activities.

B.1.12 Permitted Actions without Identification or Authentication

[Licensee/Applicant] is responsible for the following:

- identifying and documenting specific user actions that can be performed on CDAs during normal and emergency conditions without identification or authentication, and
- permitting actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives, without adversely affecting safety, security, and emergency preparedness (SSEP) functions, and in a manner consistent with NRC regulations.

B.1.13 Automated Marking

[Licensee/Applicant] is responsible for the following:

- identifying and implementing standard naming conventions for identification of special dissemination, handling, or distribution instructions in compliance with a policy and set of procedures to ensure that sensitive information is protected from inadvertent disclosure and 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," and
- ensuring that 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., Security Related Information).

B.1.14 Automated Labeling

[Licensee/Applicant] labels hard and soft copy information in storage, in process, and in transmission.

B.1.15 Network Access Control

[Licensee/Applicant] employs and documents mitigation techniques to secure CDAs through [media access control address locking, physical or electrical isolation, static tables, encryption, or monitoring].

B.1.16 "Open/Insecure" Protocol Restrictions

[Licensee/Applicant] is responsible for the following:

- documenting and implementing additional precautions to protect networks and bus communications from unauthorized access when protocols lack security controls,
- prohibiting the protocols from initiating commands except within the same boundary, and
- prohibiting these protocols from initiating commands that could change the state of the CDA from a more secured posture to a less secured posture.

B.1.17 Wireless Access Restrictions

[Licensee/Applicant] is responsible for the following:

- only allowing wireless access through a boundary security control device and treating wireless connections as outside of the security boundary,
- prohibiting the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions,
- disabling wireless capabilities when not utilized,
- establishing usage restrictions and implementation guidance for wireless technologies,
- documenting, justifying, authorizing, monitoring, and controlling wireless access to CDAs and ensuring that the wireless access restrictions are consistent with defensive strategies and defensive models, as articulated in RG 5.71, and
- conducting scans [no less frequently than once every week] for unauthorized wireless access points, in accordance with this document, and disabling access points if unauthorized access points are discovered.

B.1.18 Insecure and Rogue Connections

[Licensee/Applicant] verifies that, during deployment of CDAs, when changes or modifications have been made to CDAs, and [no less frequently than once every month], CDAs are free of insecure and rogue connections such as vendor connections and modems.

B.1.19 Access Control for Portable and Mobile Devices

[Licensee/Applicant] is responsible for the following:

- establishing and documenting usage restrictions and implementation guidance for controlled portable and mobile devices,
- authorizing, monitoring, and controlling device access to CDAs,
- enforcing and documenting that mobile device security and integrity are maintained at a level consistent with the CDA they support, and
- enforcing and documenting that mobile devices are only used in one security level and that mobile devices are not moved between security levels.

B.1.20 Proprietary Protocol Visibility

[Licensee/Applicant] ensures that, when proprietary protocols that create a lack of visibility are used (e.g., systems cannot detect attacks because the protocol is proprietary), alternative controls or countermeasures are implemented to protect the CDAs from cyber attack up to and including the design-basis threat (DBT).

B.1.21 Third Party Products and Controls

[Licensee/Applicant] ensures that for situations in which (1) third-party security solutions are not allowed because of vendor license and service agreements and (2) loss of service support would occur if third-party applications were to be installed without vendor acknowledgement or approval, alternative controls or countermeasures are implemented to mitigate vulnerabilities created by the lack of security functions provided by third-party products.

B.1.22 Use of External Systems

[Licensee/Applicant] is responsible for the following:

- ensuring that external systems cannot be accessed from higher levels, such as Levels 4 and 3,
- prohibiting external systems from accessing CDAs in Levels 3 and 4, and
- prohibiting users from using an external system to access CDAs or to process, store, or transmit organization-controlled information except in situations in which [Licensee/Applicant] verifies the implementation of equivalent security measures on the external system.

B.1.23 Publicly Accessible Content

[Licensee/Applicant] is responsible for the following:

- designates individuals authorized to post information onto a [Licensee/Applicant] system that is publicly accessible;
- trains authorized individuals to ensure that publicly accessible information does not contain information that could cause an adverse impact on SSEP functions or could assist an adversary in carrying out an attack;
- ensuring 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,

B.2 Audit and Accountability

B.2.1 Audit and Accountability Policy and Procedures

[Licensee/Applicant] developed, disseminated, and [annually] reviews and updates the following while using an independent party for the audit reviews:

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

B.2.2 Auditable Events

[Licensee/Applicant] is responsible for the following:

- determining and documenting with SSEP functions those CDAs related events that require auditing,
- defining the list of auditable events and frequency of auditing for each identified auditable event,
- at a minimum, auditing all CDA connections, user login/logouts, configuration/software/firmware changes, audit setting changes, privileged access, privileged commands, and any modifications of the security functions of CDAs,
- implementing alternative controls and documenting the justification for alternative controls and countermeasures for situations in which a CDA cannot support the use of automated mechanisms to generate audit records and employs nonautomated mechanisms and procedures,
- reviewing and updating the list of defined auditable events [no less frequently than once a year],
- including execution of privileged functions in the list of events to be audited by the CDAs,
- preventing CDAs from purging audit event records on restart,
- coordinating security audit functions within the facility to enhance mutual support and to help guide the selection of auditable events,

- configuring all CDAs so that auditable events are adequate to support after-the-fact investigations of security incidents, and
- adjusting the events to be audited within the CDAs based on current threat information and effectiveness analysis described in Section 4.1.2 of Appendix A to RG 5.71.

B.2.3 Content of Audit Records

[Licensee/Applicant] is responsible for the following:

- ensuring 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 outcomes of the events;
- ensuring that CDAs provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject; and
- implementing 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.

B.2.4 Audit Storage Capacity

[Licensee/Applicant] allocates audit record storage capacity, meets NRC record retention requirements, and configures auditing to reduce the likelihood of such capacity being exceeded.

B.2.5 Response to Audit Processing Failures

[Licensee/Applicant] ensures the following:

- 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 what the organization's resources and response times are] and documented.
- Justification and details for alternate compensating security controls are documented for those instances in which a CDA cannot respond to audit processing failures.
- Responses to audit failures by the [Licensee/Applicant] 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 [Licensee/Applicant] officials in the event of an audit processing failure.
  - Auditing failures are treated as a failure of the CDA or security boundary device and [Licensee/Applicant] will take action in accordance with the technical specification.
  - CDAs with auditing failures take the following additional actions:
    - Shut down the CDA.
    - Failover to a redundant CDA where necessary to prevent adverse impact to safety, security, or emergency preparedness functions.
    - Overwrite only the oldest audit records.
    - Stop generating audit records.

B.2.6 Audit Review, Analysis, and Reporting

[Licensee/Applicant] is responsible for the following:

- reviewing and analyzing the CDA audit records [no less frequently than once every 30 days] for indications of inappropriate or unusual activity and reporting findings to designated [Licensee/Applicant] official,
- adjusting the level of audit review, analysis, and reporting within the CDAs when there is a change in threat or risk to [Licensee/Applicant] safety, security, and emergency preparedness functions based on credible sources of information as designated by [Licensee/Applicant] or the NRC, and
- employing automated mechanisms on CDAs to integrate audit review, analysis, and reporting into [Licensee/Applicant] processes for investigation and response to suspicious activities.

B.2.7 Audit Reduction and Report Generation

[Licensee/Applicant] has configured and deployed all CDA to do the following:

- provide CDA audit reduction and report generation capability, and
- provide the capability to automatically process audit records for events of interest based upon selectable event criteria.

[Licensee/Applicant] documents the justification and details for alternate compensating security controls for situations in which a CDA cannot support auditing reduction and report generation by providing this capability through a separate system.

B.2.8 Time Stamps

[Licensee/Applicant] CDAs use a time source protected at an equal or greater level than the CDAs or an internal system clocks to generate time stamps for audit records, and [Licensee/Applicant] synchronizes the time on all CDAs.

[Licensee/Applicant] synchronizes the time of all CDAs 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.

[Licensee/Applicant] implements only methods of time synchronization that do not introduce a vulnerability to cyber attack and/or common-mode failure and implements alternative controls to manage potential cyber security risks when time synchronization can not be used for a CDA.

B.2.9 Protection of Audit Information

[Licensee/Applicant] is responsible for the following:

- protecting audit information and audit tools from unauthorized access, modification, and deletion in a manner consistent with the CDA sources, and
- ensuring that all audit information is protected at the same level as the device sources.

B.2.10 Nonrepudiation

[Licensee/Applicant] protects CDAs and audit records against an individual falsely denying they performed a particular action.

B.2.11 Audit Record Retention

[Licensee/Applicant] retains audit records consistent with the recordkeeping requirements for the access authorization program to provide support for after-the-fact investigations of security incidents and to meet regulatory and [Licensee/Applicant] record retention requirements.

B.2.12 Audit Generation

[Licensee/Applicant] security architecture provides the following:

- audit record generation capability for the auditable events on CDAs,
- audit record generation capability and the capability for authorized users to select which auditable events are to be audited by specific components of CDAs,
- audit records for the selected list of auditable events on CDAs, and
- 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 [Licensee/Applicant] defined level of tolerance for the relationship between time stamps of individual records in the audit trail.

B.3 Critical Digital Asset and Communications Protection

B.3.1 Critical Digital Asset and Communications Protection Policy and Procedures

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

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

B.3.2 Application Partitioning and Security Function Isolation

[Licensee/Applicant] is responsible for the following:

- configuring CDAs to separate applications into user functionality (including user interface services) and CDA management functionality,
- configuring CDAs to isolate security functions from nonsecurity functions, which is accomplished through [partitions, domains, etc.], including control of access to and integrity of the hardware, software, and firmware that perform these security functions,
- configuring CDAs to employ underlying hardware separation mechanisms to facilitate security function isolation,
- configuring CDAs to isolate critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and other security functions,
- configuring CDAs to minimize the number of nonsecurity functions included within the isolation boundary containing security functions,
- configuring CDA security functions as independent modules that avoid unnecessary interactions between modules,
- configuring CDA security functions as a layered structure minimizing interactions between levels of the design and avoiding any dependence by lower levels on the functionality or correctness of higher levels, and

- implementing alternative controls and documenting the justification for alternative controls or countermeasures for situations in which a CDA cannot support security function isolation and taking all of the following actions:
  - physically restrict access to the CDA,
  - monitor and record physical access to the CDA to detect and respond to intrusions in a timely manner,
  - use auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - ensure that individuals who have access to the CDAs are qualified, and
  - ensure that those individuals are trustworthy and reliable in accordance with 10 CFR 73.56.

B.3.3 Shared Resources

[Licensee/Applicant] is responsible for the following:

- configuring CDAs to prevent unauthorized and unintended information transfer via shared system resources, and
- using physically separate network devices to create and maintain logical separation of Levels 3 and 4 from each other and from all other levels.

B.3.4 Denial of Service Protection

[Licensee/Applicant] is responsible for the following:

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

B.3.5 Resource Priority

[Licensee/Applicant] configures CDAs to limit the use of resources by priority by preventing lower priority processes from delaying or interfering with the servicing of any higher priority process.

B.3.6 Transmission Integrity

[Licensee/Applicant] is responsible for the following:

- configuring CDAs to protect the integrity of transmitted information,
- employing cryptographic mechanisms to recognize changes to information during transmission and upon receipt, unless otherwise protected by alternative physical measures,
- implementing mechanisms to prevent “man-in-the-middle” (MITM) attacks via the following methods:
  - Media Access Control Address Locking—[Licensee/Applicant] locks devices and ports via address locking to prevent MITM attacks and rogue devices from being added to the network
  - Network Access Control—[Licensee/Applicant] implements network access control to prevent MITM attacks and rogue devices from being added to the network,
- implementing monitoring to detect MITM and address resolution protocol poisoning, and

- implementing alternative controls and documenting the justification for alternative controls or countermeasures for situations in which a CDA cannot support transmission integrity and implements all of the following:
  - physically restricts access to the CDA,
  - monitors and records physical access to the CDA to detect and respond to intrusions in a timely manner,
  - 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 in accordance with 10 CFR 73.56.

B.3.7 Transmission Confidentiality

[Licensee/Applicant] is responsible for the following:

- configuring the CDAs to protect the confidentiality of transmitted information,
- employing cryptographic mechanisms to prevent unauthorized disclosure of information during transmission and receipt unless otherwise protected by alternative physical measures, and
- implementing alternative controls and documenting the justification for alternative controls or countermeasures for situations in which a CDA cannot internally support transmission confidentiality capabilities, including virtual private networks, or implements all of the following:
  - physically restricts access to the CDA,
  - monitors and records physical access to the CDA to detect and respond to intrusions in a timely manner,
  - 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 in accordance with 10 CFR 73.56.

B.3.8 Trusted Path

[Licensee/Applicant] configures CDAs to use trusted communication paths between the user and the security functions of the CDAs, which includes authentication and reauthentication, at a minimum.

B.3.9 Cryptographic Key Establishment and Management

[Licensee/Applicant] manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures when cryptography is required and employed within the CDAs in accordance with [Federal Information Processing Standards (FIPS)140-2 Security Requirements for Cryptographic Modules].

B.3.10 Use of Cryptography

[Licensee/Applicant] configures CDAs to implement cryptographic mechanisms that comply with [Federal Information Processing Standards (FIPS)140-2 Security Requirements for Cryptographic Modules].

B.3.11 Unauthorized Remote Activation of Services

[Licensee/Applicant] is responsible for the following:

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

B.3.12 Transmission of Security Parameters

[Licensee/Applicant] configures CDAs to associate security parameters with information exchanged between CDAs.

B.3.13 Public Key Infrastructure Certificates

[Licensee/Applicant] issues public key certificates under a certificate policy or obtains public key certificates under a certificate policy from a provider approved by [Licensee/Applicant].

B.3.14 Mobile Code

[Licensee/Applicant] is responsible for the following:

- establishing usage restrictions and implementation guidance for mobile code technologies based on their potential to cause damage to CDAs if used maliciously, and
- authorizing, monitoring, and controlling the use of mobile code within the CDAs.

B.3.15 Secure Name/Address Resolution Service (Authoritative/Trusted Source)

[Licensee/Applicant] is responsible for the following:

- configuring systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries, and
- configuring 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.

B.3.16 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

[Licensee/Applicant] is responsible for the following:

- configuring 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, and
- configuring CDAs so that, upon receipt of data, they perform data origin authentication and data integrity verification on resolution responses whether or not the CDAs explicitly request this service.

B.3.17 Architecture and Provisioning for Name/Address Resolution Service

[Licensee/Applicant] 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).

B.3.18 Session Authenticity

[Licensee/Applicant] configures CDAs to provide mechanisms to protect the authenticity of communications sessions.

B.3.19 Thin Nodes

[Licensee/Applicant] configures CDAs and consoles to employ processing components that have minimal functionality and data storage.

B.3.20 Confidentiality of Information at Rest

[Licensee/Applicant] configures CDAs to protect the confidentiality of information at rest.

B.3.21 Heterogeneity/Diversity

[Licensee/Applicant] employs diverse technologies in the implementation of CDAs.

B.3.22 Fail in Known State

[Licensee/Applicant] is responsible for the following:

- CDAs fail in a known-state to ensure that SSEP functions are not adversely impacted by the CDAs failure, and
- to prevent a loss of confidentiality, integrity, or availability in the event of a failure of the CDA or a component of the CDA.

B.4 Identification and Authentication

B.4.1 Identification and Authentication Policies and Procedures

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

- a formal, documented identification and authentication policy, which addresses purpose, scope, roles, responsibilities, management commitments, 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 the following:

- uniquely identifying each user, and processes acting on behalf of a user,
- verifying the identity of each user, 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 after a maximum of [30 days] of inactivity,
- disabling user identifier immediately upon termination of users need for access,
- archiving user identifiers,
- defining initial authenticator content,
- establishing administrative procedures for initial authenticator distribution; lost, compromised, or damaged authenticators; and revoking authenticators,
- changing default authenticators upon control system installation, and
- changing/refreshing authenticators [annually].

B.4.2 User Identification and Authentication

[Licensee/Applicant] is responsible for the following:

- implementing identification and authentication technology to uniquely identify and authenticate individuals and processes acting on behalf of users interacting with CDA and ensuring that CDAs, security boundary devices, physical controls of the operating environment, and individuals interacting with CDAs, are uniquely identified and authenticated and that all processes acting on behalf of users are equally authenticated and identified,
- ensuring that the authentication technology employs strong multifactor authentication using protected processing levels,
- implementing alternative controls and documenting the justification for alternative controls or countermeasures for situations in which a CDA cannot support user identification and authentication and implementing all of the following:
  - physically restricting access to the CDA,
  - monitoring and recording physical access to the CDA to detect and respond to intrusions in a timely manner,
  - using auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
  - ensuring that individuals who have access to the CDA are qualified, and
  - ensuring that those individuals are trustworthy and reliable in accordance with 10 CFR 73.56,
- implementing secure domain-based authentication, as well as the following:
  - maintaining domain controllers within the given security level they are meant to service,
  - physically and logically securing domain controllers to prevent unauthorized access and manipulation,
  - prohibiting domain trust relationships between domains that exist at different security levels,
  - prohibiting domain authentication protocols from being passed between boundaries, and
  - implementing role-based access control where possible to restrict user privileges to only those required to perform the task, and
- where domain-based authentication is not used, [Licensee/Applicant] is responsible for the following:
  - documenting and justifying the reason for not implementing secure domain-based authentication,
  - implementing localized authentication when feasible,
  - implementing the strongest possible challenge-response authentication mechanism within a scenario, as supported by the application, and
  - implementing role-based access control where possible to restrict user privileges to only those required to perform the task.

B.4.3 Password Requirements

[Licensee/Applicant] ensures that, where used, passwords meet the following requirements:

- The length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the CDA.
- Passwords have length and complexity commensurate with the required security.
- Passwords are changed every [describe the periods for each class of system, for example 30 days for workstations, 3 months for CDAs in the vital area, etc. 90 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.

B.4.4 Nonauthenticated Human Machine Interaction Security

[Licensee/Applicant] is responsible for the following:

- ensuring that, for those situations in which a human machine interaction (HMI) for a CDA cannot support authentication because of operational requirements, adequate physical security controls exist that require that operators are both authorized and properly identified and are monitored so that operator actions are audited and recorded,
- controlling access to nonauthenticated human machine interactions (NHMI) so as to not hamper HMI while maintaining security of the NHMI and ensuring that access to the NHMI is limited to only authorized personnel,
- verifying that SSEP functions are not adversely affected by authentication, session lock, or session termination controls, and
- implementing auditing capability on NHMIs to ensure that all operator activity is recorded and monitored by authorized and qualified personnel and maintaining historical records to provide for auditing requirements.

B.4.5 Device Identification and Authentication

[Licensee/Applicant] is responsible for the following:

- implementing and documenting technology that identifies and authenticates devices (i.e., tester) before those devices establish connections to CDAs, and
- implementing alternative controls and documenting the justification for alternative controls or countermeasures for situations in which a CDA cannot support device identification and authentication (e.g., serial devices) and implementing all of the following:
  - physically restricting access to the CDA,
  - monitoring and recording physical access to the CDA to detect and respond to intrusions in a timely manner,
  - using auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDA,
  - ensuring that individuals who have access to the CDA are qualified, and
  - ensuring that those individuals are trustworthy and reliable in accordance with 10 CFR 73.56.

B.4.6 Identifier Management

[Licensee/Applicant] manages and documents user identifiers by performing all of the following:

- uniquely identifying each user,
- verifying the identity of each user,
- receiving authorization to issue a user identifier from an organization official,
- issuing the user identifier to the intended party,
- disabling the user identifier after a maximum of [30 days] of inactivity, and
- archiving user identifiers consistent with records retention for the access authorization program.

B.4.7 Authenticator Management

[Licensee/Applicant] manages CDA authenticators by performing all of 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; lost, compromised, or damaged authenticators; and revoking authenticators,
- changing default authenticators upon CDA installation, and
- changing/refreshing authenticators [annually].

B.4.8 Authenticator Feedback

[Licensee/Applicant] is responsible for the following:

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

B.4.9 Cryptographic Module Authentication

[Licensee/Applicant] ensures that CDAs authenticate cryptographic modules in accordance with [Federal Information Processing Standards (FIPS)140-2 Security Requirements for Cryptographic Modules].

B.5 System Hardening

B.5.1 Removal of Unnecessary Services and Programs

[Licensee/Applicant] documents all required applications, utilities, system services, scripts, configuration files, databases, and other software and the appropriate configurations, including revisions or patch levels, for each of the computer systems associated with the CDAs.

[Licensee/Applicant] maintains a list of services required for CDAs. The listing includes all necessary ports and services required for normal and emergency operations. The listing also includes an explanation or cross reference to justify why each service is necessary for operation. Only those services and programs that are necessary for operation are allowed.

[Licensee/Applicant] verifies and documents that all CDAs are patched or mitigated in accordance with the Flaw Remediation security controls in C 3.2.

[Licensee/Applicant] documents the remediation period appropriate for software and service updates or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of security.

[Licensee/Applicant] documents the operating system and software patches as CDAs evolve to allow traceability and verifies that no extra services are reinstalled or reactivated.

[Licensee/Applicant] removes or disables software components that are not required for the operation and maintenance of the CDA before incorporating the CDA into the production environment.

[Licensee/Applicant] documents components that were removed or disabled. The software removed or disabled includes, but is not limited to the following:

- device drivers for network devices not delivered,
- device drivers for unused peripherals,
- messaging services (e.g., MSN, AOL IM),
- servers or clients for unused services,
- software compilers in all 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 only during system development,
- all unused data and configuration files,
- sample programs and scripts,
- unused document processing utilities (e.g., Microsoft Word, Excel, Power Point, Adobe Acrobat, OpenOffice),
- unused removable media support, and
- games.

B.5.2 Host Intrusion Detection System

[Licensee/Applicant] establishes, implements, and documents the following requirements:

- Configure the host intrusion detection system (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 to log system and user account connections in such a way that the user or security personnel are alerted if an abnormal situation occurs.
- Configure the HIDS in a manner that does not adversely impact the CDA 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.

[Licensee/Applicant] secures HIDS configuration documents to ensure that only authorized personnel may access them.

B.5.3 Changes to File System and Operating System Permissions

[Licensee/Applicant] establishes, implements, and documents the following requirements:

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

B.5.4 Hardware Configuration

[Licensee/Applicant] establishes, implements, and documents the following requirements:

- Disable, through software or physical disconnection, unneeded networks, wireless and communication ports and removable media drives or provided engineered barriers.
- Password protect the BIOS from unauthorized changes.
- Document mitigation measures in cases for which password protection of the BIOS is not technically feasible.
- Document the hardware configuration.
- Use network devices to limit access to and from specific locations, where appropriate.
- Allow system administrators the ability to reenable devices if the devices are disabled by software and document the configuration.
- Verify that replacement devices are configured in a manner that is equal to or better than the original.

B.5.5 Installing Operating Systems, Applications, and Third-Party Software Updates

[Licensee/Applicant] establishes, implements, and documents the following:

- the patch management program, update process, and individuals responsible for installation,
- notification of vulnerabilities affecting CDAs to be conducted [within 4 hours of receipt of the vulnerability information],
- notification to authorized personnel of patches affecting cyber security,
- the authorization of updates or workarounds to the baseline before implementation,
- the patch management process for the CDA after installation, including policies, procedures, and programs relating to mitigation strategies for instances in which the vendor of the CDA informs [Licensee/Applicant] not to apply released patches, and
- the level of support for testing patch releases.

[Licensee/Applicant] establishes, implements, and tests the following:

- received cyber security updates on a nonproduction system/device for testing and validation before installing on production systems, and
- all updates for security impact.

[Licensee/Applicant] ensures that the nonproduction system/device accurately replicate the production CDA.

APPENDIX C

OPERATIONAL AND MANAGEMENT SECURITY CONTROLS

OPERATIONAL CONTROLS

C.1 Media Protection

C.1.1 Media Protection Policy and Procedures

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

- a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Site/Licensee/Applicant] entities, and compliance for each information category, as defined by the site policies, and ensures that any media which can provide information to assist an adversary is marked at a minimum to identify the sensitive nature of the media, and
- a formal, documented procedure to facilitate the implementation of the media protection policy and all associated media protection controls, including the methodology that defines the purpose, scope, roles, responsibilities, and management commitments in the areas of media receipt, storage, handling, sanitization, removal, reuse, and disposal necessary to provide 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" (SSEP) functions of the nuclear facility is prevented.

C.1.2 Media Access

[Licensee/Applicant] documents and restricts access to "critical digital asset" (CDA) media to authorized individuals only. CDA media includes both digital media (e.g., diskettes, magnetic tapes, external or removable hard drives, flash/thumb drives, compact disks, and digital video disks) and nondigital media (e.g., paper, microfilm).

[Licensee/Applicant] restricts access to any security information on mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) to authorized individuals only.

[Licensee/Applicant] employs automated mechanisms to restrict access to media storage areas and audits access attempts and accesses granted.

C.1.3 Media Labeling/Marking

[Licensee/Applicant] marks removable CDA media and CDA output 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.

C.1.4 Media Storage

[Licensee/Applicant] physically protects and securely stores CDA media to a level commensurate with the sensitivity of the data.

C.1.5 Media Transport

[Licensee/Applicant] physically protects and stores CDA media in transport in a manner commensurate with the sensitivity of the data.

[Licensee/Applicant] protects and controls CDA media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel only.

[Licensee/Applicant] protects digital and nondigital media during transport outside of controlled areas using [Licensee/Applicant]-defined security measures (e.g., locked containers, transport by security officer, cryptography).

[Licensee/Applicant] documents activities associated with the transport of CDA media using [Licensee/Applicant]-defined system of records.

[Licensee/Applicant] uses an identified custodian at all times during transport of CDA media.

C.1.6 Media Sanitation and Disposal

[Licensee/Applicant] sanitizes CDA media, both digital and nondigital, before disposal or release for reuse. [Licensee/Applicant] [follows the guidance in NIST SP 800-88] to sanitize CDA media. The information is destroyed by a method that precludes reconstruction by means available to the DBT adversaries.

[Licensee/Applicant] identifies CDA media requiring sanitization and the appropriate techniques and procedures to be used in the process; sanitizes identified CDA media, both paper and digital, before disposal or release for reuse; and implements this control so that media sanitization is consistent. [Licensee/Applicant] tracks, documents, and verifies media sanitization and disposal actions and performs [quarterly] tests on sanitized data to ensure that equipment and procedures are functioning properly.

C.2 Personnel Security

C.2.1 Personnel Security Policy and Procedures

[Licensee/Applicant]'s reviewing official grants unescorted access authorization to those individuals who have access, extensive knowledge, or administrative control of CDAs or communication systems that can adversely impact CDAs or safety, security, and emergency preparedness functions before they gain access to those systems, in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants."

C.2.2 Personnel Termination or Transfer

[Licensee/Applicant], upon termination or transfer of an individual's employment, follows the

access authorization program established under 10 CFR 73.56 and promptly performs the following actions:

- terminates all CDA and system access,
- conducts exit interviews,
- informs appropriate personnel of status change or termination,
- retrieves all security-related organizational property, and
- retains access to organizational information and CDAs formerly controlled by terminated individual.

C.3 System and Information Integrity

C.3.1 System and Information Integrity Policy and Procedures

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

- a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Licensee/Applicant] entities, and compliance, and
- formal, documented procedures to facilitate the implementation of CDAs and an information integrity policy and associated system and information integrity controls.

[Licensee/Applicant]'s system and information integrity procedures contain the following attributes:

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

C.3.2 Flaw Remediation

[Licensee/Applicant] established, implemented, and documented procedures for the following purposes:

- identifying the security alerts and vulnerability assessment process,
- communicating vulnerability information,
- correcting the flaw expeditiously utilizing the configuration management process,
- correcting security flaws in CDAs, and
- performing vulnerability scans and assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production.

Before implementing corrections, [Licensee/Applicant] documents and tests software updates related to flaw remediation to determine the effectiveness and potential side effects on CDAs. The [Licensee/Applicant] captures flaw remediation information in its Corrective Action Program.

C.3.3 Malicious Code Protection

[Licensee/Applicant] established, deployed, and documents real-time malicious code protection mechanisms 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 the following:

- data communication between systems, CDAs, removable media, or other common means, and
- exploitation of CDA vulnerabilities.

[Licensee/Applicant] documents and updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with the [Licensee/Applicant]'s configuration management policy and procedures.

[Licensee/Applicant] documents and configures malicious code protection mechanisms to ensure the following:

- Scans are performed of security boundary devices, CDAs (if applicable), workstations, servers, and mobile computing devices weekly and real-time scans of files from external sources are performed as the files are downloaded, opened, or executed.
- Infected files are disinfected and quarantined.

[Licensee/Applicant] documents and employs malicious code protection software products from multiple vendors as part of a defense-in-depth strategy and addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the CDA.

[Licensee/Applicant] centrally manages malicious code protection mechanisms to achieve the following:

- The CDAs prevent users from circumventing malicious code protection capabilities.
- The CDAs update malicious code protection mechanisms only when directed by a privileged user.

[Licensee/Applicant] does not allow users to introduce unauthorized removable media into the CDAs.

[Licensee/Applicant] disables all media interfaces (e.g., USB ports) that are not required for the operation of the CDA.

[Licensee/Applicant] documents and implements malicious code protection mechanisms to identify data containing malicious code and responds accordingly when CDAs encounter data not explicitly allowed by the security policy.

C.3.4 Monitoring Tools and Techniques

[Licensee/Applicant] is responsible for the following:

- monitoring events on the CDAs,
- detecting CDAs attacks,
- detecting and blocking unauthorized connections,
- retaining event logs in accordance with information retention requirements,
- identifying unauthorized use of the CDAs, and
- monitoring devices that are deployed to provide visibility across CDAs for the following capabilities:
  - to collect information to detect attacks, unauthorized behavior and access, and authorized access, and
  - to track specific types of transactions of interest to [Licensee/Applicant].

[Licensee/Applicant] heightens the level of monitoring activity whenever [Licensee/Applicant] or the U.S. Nuclear Regulatory Commission (NRC) determines that there is an indication of increased risk to the safety, security, or emergency operations of the site.

[Licensee/Applicant] documents, interconnects, and configures individual intrusion detection tools into a plantwide intrusion detection system using common protocols.

[Licensee/Applicant] tests cyber intrusion detection and prevention systems consistent with the timeframe defined in Nuclear Energy Institute (NEI) 03-12, Section 20.1, for intrusion detection systems, and before being placed back in service after each repair or inoperative state.

[Licensee/Applicant] documents and employs automated tools to support near-real-time analysis of events.

[Licensee/Applicant] documents and employs automated tools 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.

[Licensee/Applicant] monitors, logs, and documents inbound and outbound communications for unusual or unauthorized activities or conditions. Monitoring capabilities provide real-time alerts when indications of compromise or potential compromise occur.

[Licensee/Applicant] prevents users from circumventing intrusion detection and prevention capabilities.

[Licensee/Applicant] notifies and documents incident response personnel of suspicious events and takes the least-disruptive actions to SSEP functions to investigate and terminate suspicious events.

[Licensee/Applicant] documents and protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.

[Licensee/Applicant] uses competent cyber security personnel to randomly test and document intrusion monitoring tools.

[Licensee/Applicant] documents and makes provisions to ensure that encrypted traffic is visible to monitoring tools.

[Licensee/Applicant] analyzes and documents outbound communications traffic at the external boundary of CDAs (i.e., system perimeter) and, at selected interior points within the CDAs infrastructure to discover anomalies.

[Licensee/Applicant] ensures and documents that the use of monitoring tools and techniques does not adversely impact the functional performance of CDAs and that, where monitoring tools and techniques cannot be used, adequate alternate controls are in place to compensate.

C.3.5 Security Alerts and Advisories

[Licensee/Applicant] is responsible for the following:

- receiving timely security alerts, bulletins, advisories, and directives from credible external organizations as designated by the NRC and the [Licensee/Applicant] on an ongoing basis, such as third-party security alert notification services and vendor security alert lists, and maintaining a copy of these documents,
- independently evaluating and determining the need, severity, methods, and timeframes for implementing security directives consistent with the security controls for the CDA (Section 3.1 of Appendix A to Regulatory Guide (RG) 5.71), and
- within established timeframes set by the licensee or as directed by the NRC, [Licensee/Applicant]:
  - generates and documents internal security alerts, advisories, and directives as necessary,
  - disseminates and documents security alerts, advisories, and directives to designated personnel for action and tracks their status and completion,
  - implements and documents security directives in accordance with established timeframes or implements an alternate security measure,
  - implements and documents any required mitigation measures in accordance with the [configuration management process], and
  - employs automated or other mechanisms (e.g., e-mail lists) to make security alert and advisory information available to [Site], as needed.

C.3.6 Security Functionality Verification

[Licensee/Applicant] verifies and documents the correct operation of security functions of CDAs. This occurs, where possible, upon startup and restart, upon command by a user with appropriate privilege, [weekly], and when anomalies are discovered.

When technically feasible, CDAs provide notification of failed security tests and [Licensee/Applicant] documents these cases.

If technically feasible, CDAs provide automated support for the management of distributed security testing and [Licensee/Applicant] documents the results of this testing.

[Licensee/Applicant] documents the justification for employing alternative (compensating) controls for those situations in which a CDA cannot support the use of automated mechanisms for the management of distributed security testing. Nonautomated mechanisms and procedures to test security functions include the use of the following:

- 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 timely detection and response to intrusions), and
- auditing and validation measures (e.g., security officer rounds, periodic monitoring of tamper seals).

C.3.7 Software and Information Integrity

[Licensee/Applicant] is responsible for the following:

- 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 consistent with manufacturer or vendor recommendations, [quarterly] or as defined in NEI 03-12 or as required by NRC regulation, whichever is more frequent,
- 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 when integrity verification applications cannot be used.

C.3.8 Information Input Restrictions

[Licensee/Applicant] is responsible for ensuring the following:

- The capability to input information to CDAs is restricted to only authorized sources.
- Information is checked automatically 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 prescreened to prevent the content from being unintentionally interpreted as commands.

C.3.9 Error Handling

[Licensee/Applicant] documents and implements controls for CDAs to ensure the following:

- Error conditions are identified.

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

C.3.10 Information Output Handling and Retention

[Licensee/Applicant] retains output from CDAs to ensure that sensitive information is only disclosed to authorized personnel and is handled and disposed of to ensure that output is not disclosed to unauthorized personnel.

C.3.11 Anticipated Failure Response

[Licensee/Applicant] protects the availability of CDAs through compliance with technical specifications, preventive maintenance programs, maintenance rule programs, security plans, emergency plans, or the corrective action program. Where these programs do not apply, the availability of CDAs is provided by the following means:

- substitution of components, when needed, and a mechanism to exchange active and standby roles of the components, and
- consideration of the mean time to failure for components in specific environments of operation
- having adequate inventory of essential spare parts.

C.4 Maintenance

C.4.1 System Maintenance Policy and Procedures

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

- a formal, documented CDA maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Licensee/Applicant] entities, associated CDA maintenance controls, and compliance,
- formal, documented procedures to facilitate the implementation of the CDA maintenance policy and associated maintenance controls, and
- the system maintenance policy and procedures which cover assets located in all security boundaries, including the following:
  - owner-controlled area: the outermost protected area boundary for a plant that is outside the plant's security area,
  - protected area: an area within the boundaries of a nuclear facility that is encompassed by physical barriers and to which access is controlled (see 10 CFR 73.2, "Definitions"),
  - vital areas: areas containing any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Vital areas may also contain equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release, and
  - public access area: locations outside the physical control of the plant.

C.4.2 Maintenance Tools

[Licensee/Applicant] is responsible for the following:

- approving, monitoring, and documenting the use of CDA maintenance tools,
- inspecting and documenting maintenance tools (e.g., diagnostic and test equipment and mobile devices, such as laptops) carried into a facility by maintenance personnel for obvious improper modifications,
- checking and documenting all media and mobile devices, such as laptops, containing diagnostic, CDA, and system and test programs or software for malicious code before the media or mobile device is used in or on a CDA,
- controlling, preventing and documenting the unauthorized removal of maintenance equipment by one of the following:
  - verifying that there is no [Licensee/Applicant] information contained on the equipment and validating the integrity of the device before reintroduction into the facility,
  - sanitizing or destroying the equipment,
  - retaining the equipment within the facility, and
  - obtaining approval from an authority explicitly authorizing removal of the equipment from the facility, and
- employing [automated/manual] mechanisms to restrict the use of maintenance tools to authorized personnel only and employing manual mechanisms only when CDAs or support equipment (e.g., laptops) cannot support automated mechanisms.

C.4.3 Personnel Performing Maintenance and Testing Activities

[Licensee/Applicant] is responsible for the following:

- 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 nonautomated mechanism] to detect unauthorized use or execution of commands by an escorted individual, or designating and documenting [Licensee/Applicant] personnel with required access authorization and knowledge necessary to supervise escorted personnel interacting with CDAs.

C.5 Physical and Environmental Protection

C.5.1 Physical and Environmental Protection Policies and Procedures

For those CDAs located outside of the [Site] protected area, [Licensee/Applicant] developed, implemented, and [annually] reviews and updates the following:

- a formal, documented physical and environmental protection policy that addresses the following:
  - 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, and
  - the roles, responsibilities, and management accountability structure of the physical security program to ensure compliance with the [Licensee/Applicant] security policy and other regulatory commitments, and

- formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and operational environmental protection security controls.

C.5.2 Third Party/Escorted Access

[Licensee/Applicant] is responsible for the following:

- screening, enforcing, and documenting security controls for third-party personnel (including service contractors and other organizations providing control system operation and maintenance, development, information technology services, outsourced applications, and network and security management) and monitoring service provider behavior and compliance, and
- explicitly including personnel security controls in acquisition-related contract and agreement documents.

C.5.3 Physical and Environmental Protection

[Licensee/Applicant] secures and documents physical access to CDAs. Physical security controls (e.g., physical, locked, drivers) 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., temperature, humidity, dust, vibration and electromagnetic or radiofrequency interference).

C.5.4 Physical Access Authorizations

[Licensee/Applicant] is responsible for the following:

- 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, and
- designating officials within the organization to review and approve the above access lists and authorization credentials, consistent with the access authorization program.

C.5.5 Physical Access Control

[Licensee/Applicant] is responsible for the following:

- controlling all physical access points (including designated entry and exit points) to locations where CDAs reside and verifying individual access authorization before granting access to these areas,
- approving individual access privileges and enforcing 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 that only qualified and authorized individuals obtain access to CDAs, and
- controlling physical access to the CDAs independent of the physical access controls for the facility.

C.5.6 Access Control for Transmission Medium

[Licensee/Applicant] controls and documents physical access to CDA communication paths.

C.5.7 Access Control for Display Medium

[Licensee/Applicant] controls and documents physical access to CDAs that display information that may assist an adversary and prevents unauthorized individuals from observing the display output.

C.5.8 Monitoring Physical Access

[Licensee/Applicant] is responsible for the following:

- monitoring and documenting physical access to CDAs and security boundaries to detect and respond to physical security incidents,
- reviewing physical access logs,
- coordinating results of reviews and investigations with [Licensee/Applicant]'s 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, and
- providing adequate lighting for access monitoring devices (e.g., cameras).

C.5.9 Visitor Control Access Records

[Licensee/Applicant] is responsible for the following:

- controlling and documenting visitor physical access to CDAs by verifying the identity and confirming access authorization of these individuals prior to entry, and
- escorting visitors and monitoring visitor activity to prevent adverse impact to SSEP functions.

C.6 Defensive Strategy

[Licensee/Applicant] implements and documents its defensive strategy that identifies the protective controls associated within each security level.

[Licensee/Applicant] implements and documents a defensive model that identifies the logical boundaries for data transfer and associated communication protocols. The model defines the level of connectivity permitted between levels and individual CDAs. The elements of the defensive strategy are incorporated into CDAs. Security controls are applied commensurate with the risk associated to perform the function required to meet design specifications and operational requirements. This approach is used to deter likely methods of attack and provides high assurance of adequate protection. Defense-in-depth strategies use elements of the physical security plan; emergency response plan; and management, operation, and technical controls. Security controls are applied to CDAs to limit data flow from one level to another, thus protecting the CDA from a cyber attack originating from a less secure level. Security controls and defense-in-depth strategies are used to detect, delay, mitigate, and recover from a cyber attack.

The cyber security defensive model is deployed using a network architecture portrayed by a series of increasing defensive levels. The model takes advantage of the physical and administrative security controls implemented by the physical security program. Physical barriers such as locked doors, locked cabinets, or physical location in the [Site] protected area or vital area are also used to mitigate risk.

Section 3.2 of this plan in Appendix A documents specific information regarding the [Licensee/Applicant] defensive strategy.

C.7 Defense-in-Depth

[Licensee/Applicant] implements and documents a defensive strategy, as well as the following:

- allocates the highest degree (i.e., Level 4) of cyber security protection to CDAs that carry out safety, important to safety, and security functions and protects those CDAs from lower defensive levels,
- prevents remote access to CDAs located in the highest defensive level,
- prevents spoofing of addresses from one security level to another,
- only one-way data flow is allowed from Level 4 to Level 3 and from Level 3 to Level 2,
- initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited,
- bi-directional (2-way) communication between CDAs in Level 4 is only conducted within a security Level 4,
- any non-safety system that has bi-directional communication to a safety system is afforded the same level of protection as the safety system,
- provides intrusion prevention and detection capabilities within and at the boundaries between security levels,
- ensures for defense-in-depth levels using bi-directional (2 way) communication that data flow from one level to other levels occurs only through a device that enforces the security policy between each level and detects, prevents, delays, mitigates, and recovers from a cyber attack coming from the lower security level, and
- moves data, software, firmware, and devices from lower levels of security to higher levels of security using a documented validation process or procedure which is trustworthy at or above the trust level of the device on which the data, code, information, or device will be installed or connected with to ensure that the data, software, firmware, or devices are free from known malicious code, Trojan viruses, worms, and other passive attacks.

[Licensee/Applicant] implements and documents security boundary control devices between higher security levels and lower security levels that include the following elements:

- physically and logically secures and hardens CDAs to prevent unauthorized access or manipulation,
- employs secure management communications and encryption in accordance with Appendix B to RG 5.71,
- provides logging and alert capabilities,
- provides intrusion detection and prevention capabilities,
- detects and prevents malware from moving between boundaries,
- possesses the ability to perform more than stateful inspection with respect to the protocols used in communication across the boundary, such as through a bastion host or application proxy, and
- except in the case of data diodes, contains a rule set that at a minimum:
  - is configured to deny traffic, except that which is explicitly 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,
- is managed either through a direct connection to the firewall from a management device, such as a laptop, 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 and restricts users by allowing them to reach only the CDAs necessary for their function,
- records information flow for traffic monitoring, analysis, and intrusion detection,
- is deployed and maintained by authorized personnel adequately 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 serious cyber incidents or when directed by authorized personnel who are designated to do so,
- is evaluated, analyzed, and tested before deployment and routinely upon modification of the rule set and updates to the operational software and firmware required to operate the firewall,
- receives time synchronization from a trusted and dedicated source existing on the security network, attached directly to the CDA or via SNTP and a trusted key management process,
- synchronizes time with CDAs to provide for event correlation,
- is 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),
- routinely reviews logs by personnel that are appropriately trained in such analysis to detect malicious or anomalous activity,
- is updated [quarterly],
- uses only 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, systems, or CDAs existing at a lower security level to networks, systems, or CDAs existing at Level 4, and
- employs measures to prevent viruses or other malicious or unwanted programs from propagating information between security levels.

CDAs that provide safety, important-to-safety, security, or control functions are allocated defensive Level 4 protection. CDAs that provide data acquisition functions are allocated at least defensive Level 3 protection. The defensive model defines data transmission.

C.8 Incident Response

Measures necessary to deny, deter, and detect cyber attacks are implemented by [system, CDA, network protective devices] and align with the [Licensee/Applicant] defensive strategy.

[Licensee/Applicant] establishes, implements, and documents security controls to deny, deter, and

detect adverse threats and conditions to CDAs that may be susceptible to cyber attacks. Security controls employed counteract postulated threats. [Licensee/Applicant] establishes, implements, and documents the methods used to respond to incidents and to escalate cyber security events to the [Site/Licensee]'s incident response personnel, appropriate law enforcement authorities, or the NRC.

The [Licensee/Applicant]'s Corrective Action Program evaluates, tracks, manages, provides corrective action and documents cyber attacks.

[Licensee/Applicant] procedures that govern response to cyber events direct timely identification, detection, and response to cyber attacks. When there is a reasonable suspicion of a cyber attack, response instructions direct notification to the [shift superintendent operations, site security superintendent, manager nuclear information technology, cyber security incident response team] and other emergency response actions.

[Licensee/Applicant] procedures direct containment activities. These measures include (but are not limited to) activities necessary for the following:

- assist operations in conducting an operability determination,
- isolate the affected CDA with approval by [shift superintendent operations], if possible, and
- verify that surrounding or interconnected CDAs, networks, and support systems are not contaminated, degraded, or compromised.

Eradication activities identify the attack and the compromised pathway. [Licensee/Applicant] patches, cleans, reimages, or replaces the CDA using disaster recovery procedures. [Licensee/Applicant] governing procedures direct measures necessary to mitigate the consequences of cyber attacks.

Recovery activities include, but are not limited to, functional recovery tests, security function and requirements tests, restoration to an operational state, verification of operability, and return to active service. Systems, networks, or equipment affected by cyber attacks are restored and returned to operation as directed by [Licensee/Applicant] procedures. [Licensee/Applicant] conducts post incident analysis in accordance with its Corrective Action Program.

[Licensee/Applicant] reports cyber attacks to the NRC as directed by [Licensee/Applicant] procedures, in accordance with the requirements of Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73 and as further described in Regulatory Position C.8.6.

C.8.1 Incident Response Policy and Procedures

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

- a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Licensee/Applicant] entities, and compliance,
- formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls that establish procedures for the following:
  - 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, using the Corrective Action Program to perform an analysis to identify entry mechanisms and take steps to close down the vulnerability, and
  - establishing a disaster recovery plan that specifically permits rapid recovery from a cyber attack, including system backups which allow rapid reconstruction of the CDA, and
- recovery plans that are exercised to ensure that they are effective and that personnel are sufficiently familiar with how to employ them in accordance with [disaster recovery plans, business continuity or emergency plans] and that changes made are based on lessons learned from exercises and drills and actual incidents and events.

[Licensee/Applicant] includes stakeholders 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, and
- legal.

C.8.2 Incident Response Training

[Licensee/Applicant] is responsible for the following:

- training personnel in their incident response roles and responsibilities with respect to the CDAs and providing refresher training [at least annually],
- incorporating simulated events into incident response training to facilitate effective response by personnel in crisis situations, and
- documenting incident response training exercises and acknowledgements that personnel are qualified and trained.

C.8.3 Incident Response Testing and Drills

[Licensee/Applicant] is responsible for the following:

- testing and conducting drills of the incident response capability for CDAs [at least annually],
- using [Licensee/Applicant]-defined tests or drills or both 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 thoroughly and effectively test or drill the incident response capability, and

- performing and documenting announced and unannounced tests and drills.

C.8.4 Incident Handling

[Licensee/Applicant] is responsible for the following:

- implementing and documenting an ongoing incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery [rolled into existing incident handling program],
- incorporating lessons learned from ongoing incident handling activities into incident response procedures and implementing the procedures accordingly,
- forming an integrated cyber security incident response team (CSIRT),
- in the event of an unplanned incident that reduces the number of required cyber security personnel, compensating, by using other trained and qualified onsite cyber security personnel or calling in off-duty personnel within 2 hours from the time of discovery,
- providing the team with the technical skills and authority to effectively 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, and
- 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 each component of the Incident Response &Recovery (IR&R) process,
  - description of individual postulated classes or categories of incidents or attacks, as analyzed during attack vector analysis, and indicators and potential or planned methods of mitigation,
  - 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,
  - establishment of coordinated and secure communication methods to be used between local and remote CSIRT members and outside agencies, and
  - description of response escalation requirements.

The [Licensee/Applicant] 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 highly skilled cyber security staff member might have expertise in all of these areas.

- Nuclear facility 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.
- [Licensee/Applicant] may not have onsite personnel trained and experienced in all arenas. 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 are 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 report,
- type of incident (e.g., accident, virus),
- entry point (e.g., Internet, wireless, modem),
- perpetrator,
- type of system, hardware and software impacted,
- brief description of incident,
- impact on organization,
- measures to prevent recurrence, and
- references.

C.8.5. Incident Monitoring

[Licensee/Applicant] tracks and documents security incidents on an ongoing basis using automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

C.8.6 Incident Reporting

Regulatory Guide (RG) 5.69, "Guidance for the Application of the Radiological Sabotage Design Basis Threat in the Design, Development and Implementation of a Physical Security Protection Program that Meets 10 CFR 73.55 Requirements" (Safeguards Information), provides guidance on the type of cyber attacks and cyber security incidents that are reported to the U.S. Nuclear Regulatory Commission (NRC).

During the process to investigate and recover from a cyber security attack or cyber incident, a review to determine reportability is necessary. Currently, several regulations exist to report emergency and nonemergency events to the NRC. Reporting guidance exists but does not explicitly establish cyber security reporting criteria. The NRC has developed Draft Regulatory Guide DG-5019, "Reporting of Safeguards Events," but has not finalized or issued it at the time of this summary.

C.8.7 Incident Response Assistance

[Licensee/Applicant] provides competent and trained incident response support personnel who are available year round, 24 hours per day to offer advice and assistance to users of CDAs in response to and reporting of cyber security incidents. The support resource is an integral part of [Licensee/Applicant]'s incident response capability.

Licensee/Applicant] employs mechanisms to increase the availability of incident response-related information and support.

C.8.8 Cyber Incident Response Plan

[Licensee/Applicant] developed an incident response plan that:

- describes the structure and organization of the cyber incident response capability,
- provides a high-level approach for how the cyber incident response capability fits into the overall organization,
- defines reportable cyber incidents consistent with Regulatory Position C.8.6,
- provides metrics for measuring the cyber incident response capability within the organization,
- defines the resources and management support needed to effectively maintain and mature an incident response capability, and
- is reviewed and approved by the Cyber Security Program Sponsor.

[Licensee/Applicant] distributes copies of the incident response plan plant personnel including incident response personnel, reviews the incident response plan [annually], revises the incident response plan to address changes or problems encountered during plan implementation, execution, or testing, and communicates incident response plan changes to plant personnel including incident response personnel.

C.9 Contingency Planning/Continuity of Safety, Security, and Emergency Preparedness Functions

C.9.1 Contingency Planning Policy and Procedures

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

- a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Licensee/Applicant] entities, and compliance, and
- formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

[Licensee/Applicant] updates contingency planning policy and procedures and, where necessary, related policies and procedures for other programs when [Licensee/Applicant] review indicates updates are required.

[Licensee/Applicant]'s contingency plan includes the following:

- 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 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 or function or both) for authorized physical and cyber access to the CDA,
- communication procedure and list of personnel (according to title or function or both) to contact in the case of an emergency, and
- documented requirements for the replacement of components.

C.9.2 Contingency Plan

[Licensee/Applicant] is responsible for the following:

- implementing a cyber security contingency plan to maintain the SSEP functions by developing and disseminating roles, responsibilities, assigned individuals with contact information, and activities associated with determining the effects of CDAs after a compromise, disruption or failure and restoring those CDAs,
- coordinating contingency plan development with [Licensee/Applicant] organizations responsible for related plans (e.g., emergency plan, physical security plan) and requirements (e.g., technical specifications),
- maintaining the necessary resources and capacity to ensure that necessary information processing, telecommunications, and environmental support exist during crisis situations,
- documenting the resources needed to ensure that the capacity necessary for information processing, telecommunications, and environmental support exists during crisis situations, and
- 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.

C.9.3 Contingency Plan Testing

[Licensee/Applicant] is responsible for taking the following actions:

- tests and/or exercises and documents the contingency plan [at least annually] to verify its effectiveness and the organization's readiness to execute this plan,
- reviews the contingency plan test and exercise results and initiates appropriate corrective actions,
- coordinates contingency plan testing and/or exercises with [Licensee/Applicant] elements responsible for related plans,

- tests and/or exercises and documents 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,
- employs automated mechanisms to thoroughly and effectively test/exercise the contingency plan by providing a more complete coverage of contingency issues and selecting more realistic test/exercise scenarios and environments,
- includes recovery and reconstitution of CDAs as part of contingency plan testing,
- establishes and documents alternate controls when the contingency plan cannot be tested or exercised on production CDAs because of the potential for a significant adverse impact on safety, security, performance, or reliability of the site or CDA, and
- uses scheduled and unscheduled system maintenance activities, including responding to CDA component and system failures, as an opportunity to test or exercise the contingency plan.

C.9.4 Contingency Plan Training

[Licensee/Applicant] is responsible for the following:

- training personnel in their contingency roles and responsibilities with respect to the CDAs and providing refresher training [at least annually] or consistent with the [Licensee/Applicant's] overall contingency program, whichever period is shorter,
- maintaining training procedures and documenting training records of individuals,
- including training drills to familiarize contingency personnel with the facility, CDAs, and available resources and evaluating the site's capabilities to support contingency operations,
- employing automated mechanisms to thoroughly and effectively test/drill the contingency plan by providing more complete coverage of contingency issues, and
- selecting realistic test/drill scenarios and environments, effectively stressing the CDAs.

C.9.5 Alternate Storage Site and Location for Backups

[Licensee/Applicant] identifies and documents alternate storage locations and initiates necessary agreements to permit the storage of CDA backup information. The frequency of CDA backups and the transfer rate of backup information to the alternate storage locations are consistent with [Licensee/Applicant]'s recovery time objectives and recovery plan objectives.

[Licensee/Applicant] is responsible for the following:

- 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, and
- identifying and documenting potential accessibility problems to the alternate storage location in the event of a wide area disruption or disaster and implementing explicit mitigation actions.

C.9.6. CDA Backups

[Licensee/Applicant] is responsible for the following:

- 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 [monthly] to verify media reliability and information integrity,
- using backup information in the restoration of CDA 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 collocated with the operational software, and
- 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.

C.9.7 Recovery and Reconstitution

[Licensee/Applicant] employs mechanisms with supporting procedures that allow CDAs to be recovered and reconstituted to a known secure state following a disruption or failure and only when initiated by authorized personnel. [Licensee/Applicant] performs regression testing before returning to normal operations to ensure that CDA are performing correctly.

C.10 Awareness and Training

C.10.1 Cyber Security Awareness and Training

[Licensee/Applicant] establishes, implements, and documents the training requirements necessary for licensee/applicant personnel and contractors to perform their assigned duties and responsibilities in implementing the requirements of the program.

[Licensee/Applicant] 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.

C.10.2 Awareness Training

[Licensee/Applicant]'s 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 and information. Policy-level awareness training provides employees and contractors with the ability to understand security policies so that the program is effectively implemented. Individual users must understand their responsibility for adherence to applicable policies and standards.

[Licensee/Applicant] establishes, implements, and documents requirements for the following:

- Training programs provide basic cyber security awareness training for facility personnel. Refresher or continuous training provides updates on new threats and technology.
- Cyber security awareness is provided by displaying posters, offering security-messaged items, generating e-mail advisories and notices, and displaying logon screen messages.
- Training includes practical exercises to simulate actual cyber incidents, recovery plans, response plans and adversary attacks.

[Licensee/Applicant] develops and documents the content of cyber security training based on the

following:

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

[Licensee/Applicant] establishes, implements, and documents requirements for training to provide the following:

- cyber security awareness training for [Licensee/Applicant] employees and contractors which addresses the following:
  - the site-specific objectives, management expectations, programmatic authority, roles and responsibilities, policies, procedures, and consequences for noncompliance with the cyber security program,
  - general attack methodologies, including social engineering techniques and appropriate and inappropriate cyber security practices,
  - attack indicators, such as the following:
    - 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, and
    - unusual equipment in secure areas,
  - organizational contacts to whom to report suspicious activity, incidents, and violations of cyber security policies, procedures, or practices,
  - an explanation as to why access and control methods are required,
  - measures users can employ to reduce risks, and
  - the impact on the organization if the control methods are not incorporated.

C.10.3 Technical Training

[Licensee/Applicant] establishes, implements, and documents training programs for personnel performing, verifying, or managing activities within the scope of the program to ensure that suitable proficiency is achieved and maintained. [Licensee/Applicant] 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.

[Licensee/Applicant] establishes, implements, and documents requirements to do the following:

- provide cyber security-related technical training to individuals:
  - before authorizing access to CDAs or performing assigned duties,
  - when required by policy or procedure changes and plant modifications, and
  - annually or at an interval as defined by the [Licensee/Applicant], whichever is shorter, to mitigate risk and to ensure personnel maintain competency, and
- 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 which 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

[Licensee/Applicant] provides system managers, cyber security specialists, system owners, network administrators, and other personnel having access to system-level software with security-related technical training to perform their assigned duties.

C.10.4 Specialized Cyber Security Training

[Licensee/Applicant] 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.

[Licensee/Applicant] establishes, implements, and documents requirements for advanced training 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,
- the provision of cyber security guidance, assistance, and training for other staff members,
- the review of programmatic and system-specific cyber security plans and practices,
- assessment of CDAs, networks, and assets for compliance with cyber security policies, and
- design, acquisition, installation, operation, maintenance, or administration of security controls.

C.10.5 Cross-Functional Cyber Security Team

[Licensee/Applicant] develops, implements, and documents a cross-functional cyber security team (CST).

[Licensee/Applicant] develops, implements, and documents a program to share expertise and varied domain knowledge between members of the CST.

[Licensee/Applicant]'s CST includes, at a minimum, a member of the organization's information technology staff, an instrumentation and control system engineer, a control system operator, a subject matter expert in cyber security, and a member of the management staff.

[Licensee/Applicant]'s cyber security subject matter experts' skills include network architecture and design, security processes and practices, and secure infrastructure design and operation.

[Licensee/Applicant]'s CST also includes the control system vendor or system integrator, as needed.

[Licensee/Applicant]'s CST reports [directly to organizational structure how and who].

C.10.6 Situation Awareness

[Licensee/Applicant] security training describes the physical processes being controlled, as well as the associated CDAs and security controls.

C.10.7 Feedback

[Licensee/Applicant] establishes, implements, and documents a feedback process for personnel and contractors to refine the cyber security program and address identified training gaps.

C.10.8 Security Training Records

[Licensee/Applicant] documents and monitors individual cyber security training.

C.10.9 Contacts with Security Groups and Associations

[Licensee/Applicant] maintains contact with selected security groups to remain informed of newly recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.

C.10.10 Roles and Responsibilities

[Licensee/Applicant] creates, documents, and staffs the following positions (roles) with appropriately qualified personnel:

Role: Cyber Security Sponsor

Requirements: member of senior site management

Responsibilities:

- overall responsibility and accountability for the cyber security program, and
- provides resources required for the development, implementation and sustenance of the cyber security program.

Role: Cyber Security Program Manager

Responsibilities:

- provides oversight of the plant cyber security operations,
- functions as a single point of contact for issues related to site cyber security,
- provides oversight and direction on issues regarding nuclear plant cyber security,
- initiates and coordinates CSIRT functions as required,
- coordinates with the NRC 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.

Role: Cyber Security Specialist

Responsibilities:

- protects CDAs from cyber threat,
- understands the cyber security implications surrounding the overall architecture of plant networks, control systems, safety systems, operating systems, hardware platforms, plant-specific applications, and the services and protocols upon which those applications rely,
- performs cyber security evaluations of digital plant systems,
- conducts security audits, network scans, and penetration tests against CDAs as necessary,
- conducts cyber security investigations involving compromise of CDAs,
- preserves evidence collected during cyber security investigations to prevent loss of evidentiary value, and
- maintains expert skill and knowledge level in the area of cyber security.

Role: Cyber Security Incident Response Team

Requirements:

- personnel have knowledge of cyber forensics and
- functions in accordance with the incident response plan

Responsibilities:

- initiates emergency action when required to safeguard CDAs from compromise and to assist with the eventual recovery of compromised systems,
- contains and mitigates incidents involving critical and other support systems, and

- restores compromised CDAs.

C.11 Configuration Management

C.11.1 Configuration Management

[Licensee/Applicant] establishes, implements, and documents configuration management security controls for CDAs consistent with the process described in Section 4.2.1 of [this Plan (Appendix A)].

C.11.2 Configuration Management Policy and Procedures

[Licensee/Applicant] develops, disseminates, and [annually] reviews and updates a formal, documented configuration management policy and implementing procedures that address the purpose, scope, roles, responsibilities, management commitment, [coordination among [Licensee/Applicant] entities], associated configuration management controls, and compliance.

[Licensee/Applicant] documents its configuration management policy as a 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 structured configuration management process evaluates and controls changes to CDAs to ensure that CDAs remains secure. Before any change is implemented, [Licensee/Applicant] confirms that new vulnerabilities are not introduced.

C.11.3 Baseline Configuration

[Licensee/Applicant] develops, documents, and maintains a current baseline configuration of CDAs and their connections including the interface characteristics, security requirements, and the nature of the information communicated.. As a part of the configuration management process, [Licensee/Applicant] employs [manual/automated] mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of each CDA.

[Licensee/Applicant] documents the up-to-date baseline configurations and audits the configurations [quarterly]. Baseline configurations include [but are not limited to] a current list of all components (e.g., hardware, software), configuration of peripherals, version releases of current software, and switch settings of machine components. For each CDA, [Licensee/Applicant] maintains 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 any observations made during the course of the change.

[Licensee/Applicant] documents and maintains baseline configurations for development and test environments that are managed separately from the operational/production baseline configuration.

[Licensee/Applicant] employs a “deny-all, permit-by-exception” authorization policy to identify and authorize software permitted on [Licensee/Applicant] CDAs (i.e., white lists of authorized software). After authorized changes are implemented, [Licensee/Applicant] verifies that security features still function properly and that adequate cyber security levels are maintained.

Individuals authorized to modify CDA configurations are properly trained and qualified to

perform the modifications. [Licensee/Applicant] defines the minimum physical and logical access for the modifications. Additionally, [Licensee/Applicant] employs electronic means to monitor CDA access to ensure that only authorized systems and services are used. Furthermore, [Licensee/Applicant] documents the justification for the use of alternate (compensating) security controls for instances in which monitoring cannot be done electronically, including the following:

- physically restricting access,
- monitoring and recording physical access to enable timely detection and response to intrusions,
- employing auditing and validation measures (e.g., security officer rounds, periodic monitoring of tamper seals),
- ensuring authorized individuals are trustworthy and reliable in accordance with 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.

[Licensee/Applicant] reviews log records [no less frequently than once a quarter] in compliance with the physical security plan.

C.11.4 Configuration Change Control

[Licensee/Applicant] is responsible for the following:

- authorizing and documenting changes to CDAs
- retaining and reviewing records of CDA configuration changes and audit activities associated with CDA configuration changes and employing [manual/automated] mechanisms to:
  - document changes to CDAs,
  - notify designated approval authorities, and
  - prohibit implementation of changes until designated approvals are received and documented.

C.11.5 Security Impact Analysis of Changes and Environment

The [Licensee/Applicant]'s CST performs a security impact assessment before making changes to CDAs consistent with [Section 4.2.2 of Appendix A to RG 5.71] to manage the cyber risk resulting from the changes. The CST evaluates, documents, and incorporates into the security impact analysis any identified safety and security interdependencies.

The [Licensee/Applicant] performs and documents the security impact assessment as part of the change approval process.

C.11.6 Access Restrictions for Change

[Licensee/Applicant] defines, documents, approves, and enforces physical and logical access restrictions associated with changes to CDAs and generates, retains, and audits the record [quarterly] and when there are indications that unauthorized changes may have occurred. [Licensee/Applicant] implements its configuration management program to address discovered deviations.

[Licensee/Applicant] employs automated mechanisms to detect unauthorized changes, to enforce access restrictions and to support subsequent audits of enforcement actions.

[Licensee/Applicant] documents the justification and details for alternate (compensating) security controls for situations in which a CDA cannot support the use of automated mechanisms to enforce access restrictions and to support subsequent audits of enforcement actions, including all of the following:

- physically restricting access,
- monitoring and recording physical access to enable timely detection and response to intrusions,
- employing auditing and validation measures (e.g., security officer rounds, periodic monitoring of tamper seals),
- ensuring authorized individuals are trustworthy and reliable in accordance with 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.

C.11.7 Configuration Settings

[Licensee/Applicant] applies configuration settings for CDAs by (1) documenting the most restrictive mode, (2) evaluating operational requirements, and (3) enforcing and documenting the most restrictive operational configuration settings based upon explicit operational requirements. This is achieved by the following:

- 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 and monitoring and controlling changes to the configuration settings in accordance with [Licensee/Applicant] policies and procedures,
- documenting and employing automated mechanisms to [centrally] manage, apply, and verify configuration settings,
- documenting and employing [automated mechanisms/manual mechanisms] to respond to unauthorized changes to [Licensee/Applicant]-defined configuration settings, and
- documenting the justification for alternate (compensating) security controls for situations in which a CDA cannot support the use of automated mechanisms to [centrally] manage, apply, and verify configuration settings, including all of 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 in accordance with 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.

C.11.8 Least Functionality

[Licensee/Applicant] configures and documents CDA configuration settings to provide only essential capabilities and specifically prohibits, protects, and restricts the use of insecure functions, ports, protocols and services. [Licensee/Applicant] reviews CDAs [monthly] to identify and eliminate unnecessary functions, ports, protocols, and services. [Licensee/Applicant] documents and employs automated mechanisms to prevent program execution. [Licensee/Applicant] uses [white-lists, black-lists, gray-lists] application control technologies.

C.11.9 Component Inventory

[Licensee/Applicant] develops, documents, and maintains an inventory of the components of CDAs that has the following attributes:

- accurately reflects the current system configuration,
- ensures that the location (logical and physical) of each component is consistent with the authorized boundary of the CDA,
- provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability,
- updates the inventory of system components as an integral part of component installations and system updates,
- employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of system components,
- employs automated mechanisms to detect the addition of unauthorized components or devices into the environment and disables access by such components or devices or notifies designated [Licensee/Applicant] officials, and
- documents the [names or roles] of the individuals responsible for administering those components.

MANAGEMENT CONTROLS

C.12 System and Service Acquisition

C.12.1 System and Services Acquisition Policy and Procedures

[Licensee/Applicant] develops, disseminates, and [annually] reviews and updates a formal, documented system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, [coordination among [Licensee/Applicant] entities], associated system and service acquisition controls, and compliance.

[Licensee/Applicant] develops, disseminates, and [annually] reviews and updates formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

C.12.2 Supply Chain Protection

[Licensee/Applicant] protects against supply chain threats and vulnerability by employing the

following list of measures to protect against supply chain threats to maintain the integrity of the CDAs that are acquired:

- establishment of trusted distribution paths,
- validation of vendors, and
- requiring tamper proof products or tamper evident seals on acquired products.

[Licensee/Applicant] performs an analysis for each product acquisition to determine that the product provides the security requirements necessary to address the security controls in Appendixes B and C to RG 5.71.

[Licensee/Applicant] uses heterogeneity to mitigate vulnerabilities associated with the use of a single vendor's product.

C.12.3 Trustworthiness

[Licensee/Applicant] requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

[Licensee/Applicant] establishes, implements, and documents requirements to require all tools used to perform cyber security tasks or SSEP functions to undergo a commercial qualification process similar to that for software engineering tools that are used to develop digital instrumentation and control systems.

C.12.4 Integration of Security Capabilities

[Licensee/Applicant] documents and implements a program to ensure that new acquisitions contain security design information, capabilities or both to implement security controls in Appendix B to RG 5.71. Such security capabilities include the following:

- being cognizant of evolving cyber security threats and vulnerabilities,
- being cognizant of advancements in cyber security protective strategies and security controls,
- conducting analyses of the effects that each advancement could have on the security, safety, and operation of critical assets, systems, CDAs, and networks and implementing these advancements in a timely manner, and
- replacing legacy systems as they reach end of life with systems that incorporate security capabilities.

[Licensee/Applicant] establishes timeframes to minimize the time it takes to deploy new and more effective protective strategies and security controls.

C.12.5 Developer Security Testing

[Licensee/Applicant] documents and requires that system developers and integrators of acquired CDAs create, implement, and document a security test and evaluation plan to ensure that the acquired products meet all specified security requirements (1) that the products are free from known, testable vulnerabilities and malicious code by identifying and eliminating these following vulnerabilities and other vulnerabilities that may change with new technology:

- weak, unproven, or nonstandard cryptographic modules,

- insecure network protocols for sensitive communications,
- known insecure software components or libraries,
- known vulnerabilities,
- insecure configuration files or options that act to control features of the application,
- inadequate or inappropriate use of access control mechanisms to control access to system resources,
- inappropriate privileges being granted to users, processes, or applications,
- weak authentication mechanisms,
- improperly or failing to validate input and output data,
- insecure or inadequate logging of system errors or security-related information,
- inadequately bounded buffers,
- format string vulnerabilities,
- privilege escalation vulnerabilities,
- unsafe database transactions,
- unsafe use of native function calls,
- hidden functions and vulnerable features embedded in the code,
- implemented security features do not themselves act to increase the risk of security vulnerabilities, increase susceptibility to cyber attack, or reduce the reliability of design-basis functions.
- use of unsupported or undocumented methods or functions, and
- use of undocumented code or malicious functions that might allow either unauthorized access or use of the system or the system to behave beyond the system requirements.

(2) and developers cyber security program maintains the integrity of the acquired system until the product is delivered to the [Licensee/Applicant] by implementing equivalent security controls as described in RG 5.71 to prevent tampering and to provide high assurance that the integrity of the developed CDA is maintained until delivered to the licensee.

[Licensee/Applicant] requires the developer to perform and document that security requirements are verified and validated and that security controls implemented in the product and used to meet the requirements of this plan are tested to ensure they are effective per section A.4.1.2.

[Licensee/Applicant] requires documentation of all of the following activities:

- system design transformed into code, database structures, and related machine executable representations,
- hardware and software configuration and setup,
- software coding practices and testing,
- communication configuration and setup (including the incorporation of reused software and commercial off-the-shelf products),
- The results of unit tests performed to ensure that the code was developed correctly and accurately and completely reflects the security design configuration transformations from the requirements,
- details of the implementation of each required security feature within the developed code base. The listing includes reference the coded functions and modules within the code base that were developed to implement the security features,

- security configurations implemented to meet security design features specified in the requirements,
- operating system security configurations implemented to meet security design features specified in the requirements are documented,
- For programming languages that support static analysis source code scanners, results of the following are documented:
  - the static source code vulnerability analysis performed to inspect the developed code for potential security defects, poor programming practices, hidden functions, and vulnerable features within the code during the implementation of the code base and methods applied to eliminate these vulnerabilities,
  - the security defect tracking metrics used to capture and track the identification, type, classification, cause, and remediation of security defects found within the code, and
  - the defects encountered during the translation of the design features specified in the requirements into code.
- For all programming languages, the results of the following are documented:
  - a dynamic source code vulnerability analysis performed to inspect the developed code for potential security defects, poor programming practices, hidden functions, and vulnerable features within the code during the implementation of the code base and methods applied to eliminate these vulnerabilities,
  - the security defect tracking metrics used to capture and track the identification, type, classification, cause, and remediation of security defects found within the code, and
  - the defects encountered during the translation of the design features specified in the requirements into code.

[Licensee/Applicant] requires that CDA developers/integrators:

- perform configuration management during CDA design, development, implementation, and operation,
- manage and control changes to the CDA,
- implement only [Licensee/Applicant] approved changes,
- document approved changes to the CDA, and
- track security flaws and flaw resolution.

C.12.6 Licensee/Applicant testing

[Licensee/Applicant] verifies and validates the results of the developer's security testing in conducted in accordance with Section 12.5 above.

[Licensee/Applicant] is responsible for the following:

- testing CDA (e.g., offline on a comparable CDA) security devices, security controls, and software to ensure that they do not compromise the CDA or the operation of an interconnected CDA operation before installation,
- testing to ensure that CDAs do not provide a pathway to compromise the CDA or other CDAs,
- implementation of the security controls in Appendices B and C to RG 5.71 in accordance with the process described in Section 3.1.6 of Appendix A to RG 5.71,

- testing of the security controls for effectiveness, as described in Section 4.1.2 of Appendix A to RG 5.71,
- performance of vulnerability scans, in accordance with Section 4.1.3 of Appendix A to RG 5.71 and Section 13.1 of this plan, against the CDA in its integrated state and correction, elimination, or discussion of discovered vulnerabilities,
- installation and testing of the CDA in the target environment, and
- performance of an acceptance review and test of the CDA security features.

[Licensee/Applicant] documents the following:

- Security controls implemented in accordance with Appendix B of RG 5.71.
- Verification of the effectiveness of the security controls implemented in accordance with Appendix C.
- Security design features developed to address the identified security requirements for the CDA (if any), in addition to the security controls implemented in accordance with Appendix B to 5.7.1. For each security feature or configuration to be implemented, the documentation includes a description of the feature, its method of implementation, and any configurable options associated with the feature are provided. Each security feature designed into the system is traceable to its corresponding security requirement.

The security reviews of the implemented design by the cyber security organization responsible for the protection of the critical assets/systems/networks are documented. The review ensures that the security design configuration item transformations from the requirements implemented are correct, accurate, and complete.

[Licensee/Applicant] requires [annual] audits of CDAs to verify the following:

- The security controls present during testing remain in place and are functioning correctly in the production system.
- CDAs are free from known vulnerabilities and security compromises and continue to provide information on the nature and extent of compromises, should they occur.
- The change management [process/program] is functioning effectively and is recording configuration changes appropriately.

C.13 Security Assessment and Risk Management

C.13.1 Threat and Vulnerability Management

[Licensee/Applicant] does the following:

- Perform assessments and scans for vulnerabilities in CDAs [no less frequently than once a quarter] and at random intervals in accordance with Section 4.1.3 of Appendix A to RG 5.71 and when new potential CDA vulnerabilities are reported or identified.
- Employ vulnerability scanning tools and techniques that promote interoperability among tools and automating parts of the vulnerability management process by:
  - enumerating platforms, software flaws, and improper configurations,
  - formatting and making transparent checklists and test procedures, and
  - measuring vulnerability impacts.

- Analyze vulnerability scan reports and remediate vulnerabilities within a time period that will provide high assurance that CDAs are protected from cyber attacks up to and including the DBT.
- Eliminate similar vulnerabilities in other CDAs.
- Employ vulnerability scanning tools that include the capability to update the list of cyber vulnerabilities scanned and update the list of CDA vulnerabilities scanned [monthly] and when new vulnerabilities are identified and reported.
- Employ vulnerability scanning procedures that maximize the breadth and depth of coverage (i.e., CDA components scanned and vulnerabilities checked).
- Discern and document what information associated with the CDA is discoverable by adversaries.
- Perform security testing to determine the level of difficulty in circumventing the security controls of the CDA. [Testing methods include penetration testing, malicious user testing, and independent verification and validation.]
- Include privileged access authorization to CDAs for selected vulnerability scanning activities to facilitate more thorough scanning.
- Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in CDA vulnerabilities and mitigation/flaw remediation activities.
- Employ automated mechanisms to detect and notify authorized personnel of the presence of unauthorized software on CDAs.
- Ensure that SSEP functions are not adversely impacted by the scanning process. Where this may occur, CDAs are removed from service or replicated (to the extent feasible) before scanning is conducted or be scheduled to occur during planned CDA outages whenever possible. Where [Licensee/Applicant] cannot conduct vulnerability 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) are employed.

The [Licensee/Applicant] reviews historic audit logs to determine if a vulnerability identified in the CDA has been previously exploited.

C.13.2 Risk Mitigation

Protection and mitigation of risk are achieved by implementing (1) the defense-in-depth strategies discussed in Section 3.2 of to RG 5.71, (2) the security controls described in Appendices B and C to RG 5.71, and (3) digital equipment and software cyber attack detection, prevention, and recovery techniques and tools to the systems, structures, and components within the scope of the rule and (4) Section 4 of Appendix A of RG 5.71. [Licensee/Applicant] has the detailed information on how these requirements are implemented to achieve the high assurance objectives of security controls specified in this plan. The detailed information is available for NRC inspections and audits.

C.13.3 Corrective Action Program

[Licensee/Applicant] established, implemented, and documented the criteria consistent with RG 5.71 for adverse conditions and the requirements for corrective action. The adverse impact resulting from a cyber security incident is evaluated, tracked, and adjusted in accordance with the [Licensee/Applicant] Corrective Action Program and in a manner consistent with RG 5.71.