U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5061, Rev. 1

Proposed Revision 1 to Regulatory Guide 5.71

Issue Date: July 2021
Technical Lead: Kim Lawson-Jenkins

CYBER SECURITY PROGRAMS FOR NUCLEAR POWER REACTORS

A. INTRODUCTION

Purpose

This regulatory guide (RG) provides an approach that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for complying with the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks" (Ref. 1).

Applicability

This RG applies to operating power 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).

Applicable Orders and Regulations

- 10 CFR Part 73, "Physical Protection of Plants and Materials," prescribes requirements for the establishment and maintenance of a physical protection system that will be capable of protecting special nuclear material at fixed sites and in transit as well as at plants that use special nuclear material.
    - 10 CFR 73.1, "Purpose and Scope," describes the design-basis threats (DBTs) that shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of radiological material.

Pre-Decisional

This RG is being reissued in draft form to involve the public in the development of regulatory guidance in this area. It has not received final staff review or approval and does not represent an NRC final staff position. Public comments are being solicited on this DG and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal rulemaking Web site, http://www.regulations.gov, by searching for draft regulatory guide DG-5061, Rev. 1. Alternatively, comments may be submitted to the Office of Administration, Mailstop: TWFN 7A-06M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Program Management, Announcements and Editing Staff. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this DG, previous versions of DGs, and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at https://nrcweb.nrc.gov/reading-rm/doc-collections/reg-guides/. The DG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML21095A329. The regulatory analysis may be found in ADAMS under Accession No. ML21130A636.

- 10 CFR 73.54 contains the requirements for a cyber security program for nuclear power plant (NPP) licensees that provides high assurance [1](Ref. 4) that digital computers and communication systems and networks are adequately protected against cyber attacks.

- 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," contains the requirements for establishing and maintaining a physical protection program that provides 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.

- 10 CFR 73.77, "Cyber Security Event Notifications," stipulates the types of cyber attacks that require notification to the NRC, the timeliness for conducting the notifications, how licensees should conduct the notifications, and how to submit follow up written reports to the NRC.

- NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," dated February 25, 2002 (Ref. 5), identifies the perceived threat environment that arises from computer and communication networks for safety and security vulnerabilities, including modem access vulnerabilities, as of the order's issue date.

- NRC Order EA-03-086, "Design Basis Threat for Radiological Sabotage," issued April 29, 2003 (Ref. 6), supplements the DBT for NPPs as specified in 10 CFR 73.1 and, in part, requires licensees to address additional cyber attack characteristics.

Historically, the Commission has issued a series of security orders (e.g., EA-02-026 and EA-03-086) to reactor licensees describing the protection of electronic devices and computer networks from cyber security threats. The NRC has not codified these requirements in the CFR due to the sensitivity of the security-related information. For future NPPs, the staff anticipates that, immediately following the issuance of an operating license, the NRC will issue similar orders to the licensee containing similar requirements.

Related Guidance

- RG 5.83, "Cyber Security Event Notifications" (Ref. 7), describes approaches and methodologies that the NRC staff considers acceptable for use by nuclear power reactor licensees when categorizing certain cyber security events and the process for notifying the NRC and submitting written security follow-up reports for cyber security events.

- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 8), provides specific guidance to NPP licensees for use in the design, development, and implementation of protection measures for digital instrumentation and controls used in safety-related applications.

---

1 The general performance objective of 10 CFR 73.55(b)(1) 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 the public health and safety." In SRM-SECY-16-0073, Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088, the Commission stated that "the concept of 'high assurance' of adequate protection found in our security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate" Throughout this publication of Revision 1, the term high assurance is used in alignment with Commission policy statements (*See* Ref. 4) that high assurance is equivalent to reasonable assurance of adequate protection.

Pre-Decisional

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by a basis for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG contains voluntary information collections covered by 10 CFR Parts 50, 52 and 73 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), under control number 3150-0011, 3150-0151 and 3150-0002. Send comments regarding this information collection to the Information Services Branch, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202 (3150-0011, 3150-0151 and 3150-0002), Office of Management and Budget, Washington, DC, 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

Pre-Decisional

TABLE OF CONTENTS

A. INTRODUCTION **1**

B. DISCUSSION **5**

C. STAFF REGULATORY GUIDANCE **11**

- **C.1 General Requirements** **11**
- **C.2 Elements of a Cyber Security Plan** **11**
- **C.3 Establishing and Implementing a Cyber Security Program** **13**
- **C.4 Maintaining the Cyber Security Program** **37**
- **C.5 Records Retention and Handling** **47**

D. IMPLEMENTATION **48**

GLOSSARY **49**

ACRONYMS AND ABBREVIATIONS **55**

REFERENCES **56**

BIBLIOGRAPHY ..... Error! Bookmark not defined.

APPENDIX A **A-1**

APPENDIX B **B-1**

APPENDIX C **C-1**

Pre-Decisional

B. DISCUSSION

Reason for Revision

This revision of RG 5.71, Revision 1) incorporates lessons learned from operating experience since original publication the guide. Specifically, this revision clarifies issues identified from cyber security milestone inspections, additional insights gained through the Security Frequently Asked Questions process, documented cyber security attacks, new technologies, and new regulations. Also, this revision considers the changes in the most recent revision to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, issued September 2020 (Ref. 9), as RG 5.71, Revision 0 (Ref. 10), was based on an early revision of SP 800-53.

On October 21, 2010, the Commission issued Staff Requirements Memorandum (SRM)-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants" (Ref. 11), in which the Commission determined, as a matter of policy, that the NRC's cyber security regulation (10 CFR 73.54) should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety at NRC-licensed NPPs. This decision determined that digital assets previously covered by cyber security regulations of the Federal Energy Regulatory Commission would now be covered by the NRC's cyber security regulations in 10 CFR 73.54. As a result of this policy determination by the Commission, the licensees updated their cyber security plans (CSPs) to incorporate BOP systems. This revision to RG 5.71 provides guidance for addressing SSCs associated with digital assets in the BOP falling within the scope of the NRC's cyber security regulations.

In 2015, the NRC published 10 CFR 73.77 and its associated guidance, RG 5.83, on cyber security event notifications. This rule established requirements clarifying the types of cyber attacks that require notification to the NRC, the timeliness for making the notifications, how licensees are to make notifications, and how they are to submit follow-up written reports to the NRC. This revision to RG 5.71 includes references to the NRC's guidance for cyber security event notifications.

The NRC has updated this RG to provide more guidance on risk-informed security approaches for CSP implementation.

Background

An NPP licensee's physical protection programs must comply with the performance objectives and requirements outlined in 10 CFR 73.55. The rule in 10 CFR 73.55(b)(8) requires these licensees to establish, maintain, and implement cyber security programs in accordance with 10 CFR 73.54. A licensee's cyber security program must provide high assurance that digital computer and communication systems and networks identified in 10 CFR 73.54(a)(1) are adequately protected against cyber attacks. Throughout this publication of Revision 1, the term high assurance is used in alignment with Commission policy statements that high assurance is equivalent to reasonable assurance of adequate protection. The cyber security program is part of the licensee's site physical protection program. 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.

Pre-Decisional

In response to the terrorist attacks of September 11, 2001, and subsequent information provided by intelligence and law enforcement agencies, the NRC issued Order EA-02-026 in February 2002 to address the threat environment at the time. This order includes a specific requirement directing NPP licensees to address certain cyber security vulnerabilities.

The NRC issued Order EA-03-086 in April 2003. This order supplemented the DBT for NPPs as specified in 10 CFR 73.1 and, in part, required licensees to address additional cyber attack characteristics. The substantive requirements of NRC Orders EA-02-026 and EA-03-086 contain safeguards information as defined in 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements," and are, therefore, withheld from public disclosure.

In addition, in recognition of the potential cyber-security-related issues resulting from the increased use of digital technology at NPPs, the NRC published NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," in October 2004 (Ref. 12). 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," Revision 1, dated November 18, 2005 (Ref. 13), 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. 14) informed NEI that NEI 04-04, Revision 1, provided an acceptable approach to formulating an interim cyber security program. At the time of its evaluation of NEI 04-04, the NRC had not yet proposed comprehensive cyber security regulations. RG 5.71, Revision 0, issued in 2009, provided a comprehensive approach to complying with 10 CFR 73.54 for cyber security by using strategies in the then current version of NIST SP 800-53. NUREG/CR-7141, "The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors," issued November 2014 (Ref. 15), provides an overview and historical perspective of the development of RG 5.71.

In July 2011, the NRC published Revision 3 of RG 1.152 to provide specific guidance to NPP licensees for use in the design, development, and implementation of protection measures for digital instrumentation and controls 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. 16). Revision 3 of RG 1.152 contains regulatory criteria for the evaluation of safety systems to ensure that identified security features are appropriately incorporated into systems and that the development environment is protected against the introduction of undocumented, unwanted code and any other coding that could adversely impact the operation of the safety systems. Any acquisition or modification of digital safety systems or any licensing of new reactor safety systems (one subset of the critical digital assets (CDAs) covered by RG 5.71) are reviewed through review licensing actions (such as a license amendment request, operating license application, design certification application or combined license (COL) application as described in 10 CFR Part 50 and 10 CFR Part 52). In Revision 3 of RG 1.152, regulatory positions C.2.1 through C.2.5 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 through the use of design features, it then submits the details of any design features of the safety system, intended to meet a cyber security provision of 10 CFR 73.54, 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.

Pre-Decisional

The Commission establishes requirements for the physical protection program of a nuclear power reactor facility in 10 CFR 73.55(b). 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.

Since the publication of Revision 0 of RG 5.71, the NEI has published guidance to assist licensees in implementing cyber security programs at NPPs. In April 2010, it developed NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6 (Ref. 17), to assist licensees in constructing and implementing their CSP license submittals required by 10 CFR 73.54. In July 2012, the NEI published NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2 (Ref. 18). The NRC issued a letter on June 27, 2012 (Ref. 19), stating that NEI 10-04, Revision 2, was acceptable for use by licensees to identify critical digital systems and CDAs with two exceptions. The first exception was that NEI 10-04, Revision 2, incorrectly excluded digital computing systems related to licensees' security programs. The second exception was text on support systems and equipment that could be misinterpreted to exclude systems such as digital test and maintenance equipment for safety and safety-related systems from the scope of 10 CFR 73.54. The exception in the letter stated that these systems are within the scope of the cyber security rule.

In August 2017, the NEI published NEI 13-10, "Cyber Security Control Assessment," Revision 6 (Ref. 20), to streamline the process for addressing the application of cyber security controls to the large number of CDAs identified by licensees when conducting the analysis required by 10 CFR 73.54(b).

RG 5.71 provides guidance to applicants and licensees on acceptable methods for satisfying the requirements of 10 CFR 73.54. The information contained within this RG represents the results of research conducted by the NRC 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 RG takes into account the findings by consensus 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 contains regulatory positions that promote a defensive strategy consisting of a defensive architecture and a set of tailored security controls based on standards provided in the then current versions of NIST SP 800-53 and NIST SP 800-82, "Guide to Industrial Control Systems Security," (Ref. 21). 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 safety, security, and emergency preparedness (SSEP) functions, public health and safety might be at risk. Consequently, the NRC developed this RG 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 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 that licensees should adopt to satisfy the regulatory

Pre-Decisional

requirement to defend digital assets from cyber attack up to and including the DBT, as defined in 10 CFR 73.1.

This RG 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 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 RG.

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 RG is to tailor 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.

Applicants should consider this guidance when preparing a cyber security plan (CSP) consistent with the requirements in 10 CFR Part 50 and 10 CFR Part 52. Licensees and applicants bear the sole responsibility for assessing and managing the potential for adverse effects from a cyber attack on critical digital assets associated with SSEP functions. Licensees and applicants should direct their questions on regulatory requirements for the protection of digital computer and communication systems and networks to the appropriate NRC Headquarters or regional office staff.

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 of this guide is an overview of the regulatory requirements relevant to cyber security. Section C.2 of this guide introduces the elements of a security plan and provides an acceptable method for the development of a CSP that will comply with the provisions of 10 CFR 73.54.

Section C.3 of this guide describes 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.3 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 SP 800-82 by listing security controls to address the potential cyber risks to a CDA. 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, issued July 2002" (Ref. 22), and NIST SP 800-37, "Guide to Certification and Accreditation of Federal Information Systems," issued May 2004 (Ref. 23). Section C.3 also describes an acceptable method for implementing the security controls, as detailed in Appendices B and C to this RG.

Section C.4 of this guide discusses the need to maintain the cyber security program 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 provides licensees and applicants with guidance for retaining records associated with their cyber security programs.

Pre-Decisional

Appendix A to RG 5.71 is a template for a generic CSP that 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 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.

Implementation of a cyber security plan protects CDAs that perform SSEP functions at an NPP. Assessments of identified CDAs - including attack surface, attack pathway, vulnerability, and threat information – provide the basis for selection of security controls applied to the CDAs or to the environment in which the CDAs operate. Once applied, the security controls should be continuously monitored for effectiveness. Implementation of continuous monitoring is an element of a CSP that supports timely detection of a cyber attack as required by 10 CFR 73.54 (e)(2)(i). This overview of a CSP implementation process is illustrated in Figure 1.

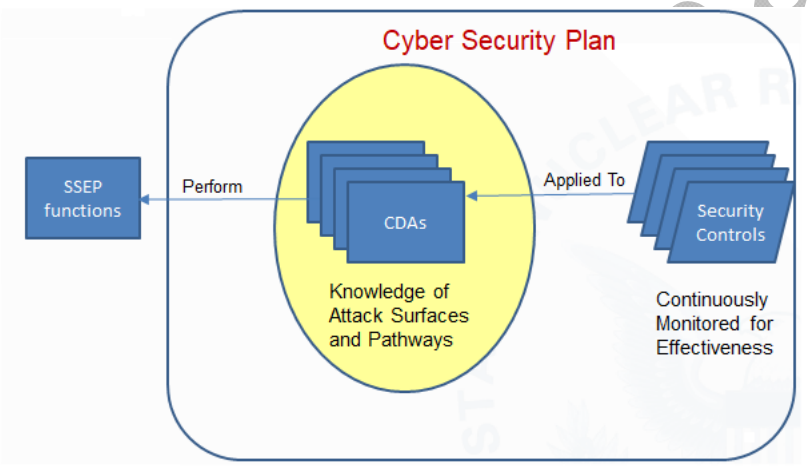

Figure 1 – Mapping CSP Effectiveness to SSEP Function Protection

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA develops Safety Requirements and Safety Guides for protecting people and the environment from harmful effects of ionizing radiation. This system of safety fundamentals, safety requirements, safety guides, and other relevant reports, reflects an international perspective on what constitutes a high level of safety. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission's International Policy Statement (Ref. 24) and Management Directive and Handbook 6.6, "Regulatory Guides (Ref. 25).

The following IAEA Safety Requirements and Guides were considered in the development/ update of the Regulatory Guide:

- IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," issued December 2011 (Ref. 26), contains guidance for incorporating computer security as a fundamental part of the overall security plan for nuclear facilities.

- IAEA Nuclear Energy Series NR-T-3.30, "Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants," issued December 2020 (Ref. 27), defines the key concepts for computer security for instrumentation and control systems at nuclear facilities, explains the risk-informed approach to computer security, and describes how computer security measures are applied throughout the instrumentation and control system life cycle.

Pre-Decisional

C. STAFF REGULATORY GUIDANCE

This RG describes methods acceptable to the NRC staff for establishing a cyber security program at a commercial NPP to comply with the Commission's regulations for adequately protecting digital computer and communication systems and networks against cyber attacks, up to and including the DBT as described in 10 CFR 73.1. This RG also provides guidance on the development of a CSP and examples of its security controls.

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 and certain support systems and equipment, which, if compromised, would adversely impact the SSEP functions of a nuclear facility. This includes 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 adversely impact 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 CSP that satisfies the cyber security program requirements of this regulation. Additionally, the CSP must describe how the licensee will implement the requirements of the regulation, taking into account site-specific conditions that affect implementation, to provide high assurance that the plan protects all SSEP functions from cyber attacks. This section lists the necessary elements of a CSP, as required by the rule.

In accordance with 10 CFR 73.54(e)(1), the CSP describes 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 includes a generic template that can be used to develop a CSP and to establish and maintain a program that will comply with this regulation.

The CSP should describe the measures and governing procedures that ensure the plan, associated records, and implementing policies and procedures meet the NRC's requirement for protection of safeguards information, as stated in 10 CFR 73.21 and 10 CFR 73.22. Revisions to the CSP are processed in accordance with 10 CFR 50.54(p).

The CSP describes 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 CSP describes 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 function
    - security functions

Pre-Decisional

- 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 establishes, 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 process for evaluating modifications to assets using 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 provides additional guidance for the design and development process of safety systems)

Pre-Decisional

- how to make a cyber security event notification in accordance with the provisions of 10 CFR 73.77 (10 CFR 73.54(d)(4))

- 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 CSP, which must be maintained at the site, and that are subject to periodic NRC inspection (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 that 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 SSEP 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 in Section C.3.3 of this guide.

As required by 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8), an NPP 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 of this guide describe an acceptable method for establishing, implementing, and maintaining a cyber security program to comply with the regulations. Figure 2 illustrates the process of establishing, implementing, and maintaining the cyber security program.

Pre-Decisional

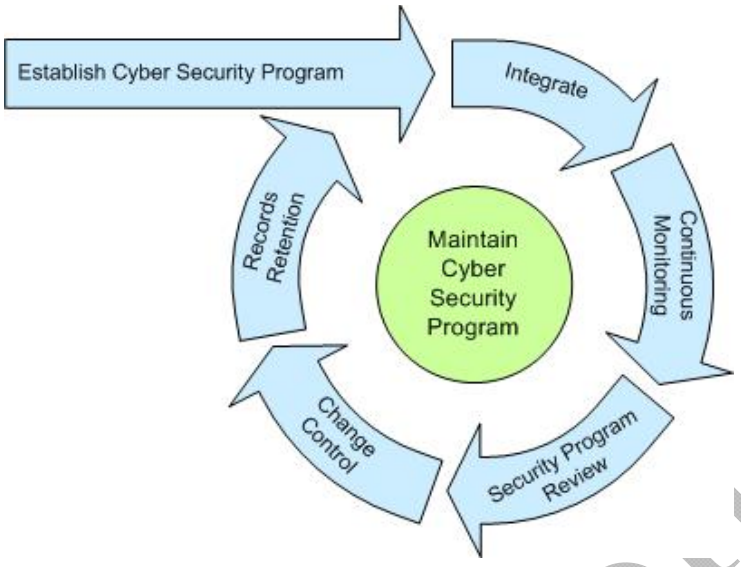

Figure 2 – Security life cycle process

An acceptable method to establish a cyber security program at a facility is by performing the following:

- analyze the digital computer and communication systems and networks;
- review the CDAs, as described in Section C.3.1.4;
- deploy defensive architecture, as described in Section C.3.2.1;
- address potential cyber risks to CDAs, as described in Section C.3.3; and
- implement the security life cycle activities in Section C.4 to maintain the cyber security program.

Such a cyber security program can be characterized as risk-informed security in that the development and maintenance of the program makes use of risk insights—including threat information, the likelihood of adversary success, and the resulting level of consequences of the threats—up to and including the DBT described in 10 CFR 73.1. Establishment of a cyber security program could include the following:

- characterization of facility functions, including the identification of SSEP functions
- characterization of threats to the facility
- specification of requirements (including the CSP, the defensive architecture, and defense-in-depth methodology)
- implementation of the requirements based on consequence analyses
- validation and verification of the implementation of 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. CDAs are those

Pre-Decisional

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 of cyber personnel and form the cyber security team (CST);
- identify and document CDAs at the facility; and
- review and validate configurations of CDAs.

Section A.3.1 of Appendix A to this document includes 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 periodically 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 RG; and

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

Section A.3.1.1 of Appendix A to this document contains a template for licensees to use in preparing the aspect of their CSP that 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 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 five categories of individuals:

- a cyber security program sponsor who is a member of senior site management (executive or officer level), has overall responsibility and accountability for the cyber security program, and provides the necessary resources for its development, implementation, and 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 on cyber security

Pre-Decisional

- initiating and coordinating cyber security incident response team (CSIRT) functions, as required
- coordinating with the NRC, DHS, U.S. Department of Energy, and the Federal Bureau of Investigation, as required, during and after cyber security incidents and events
- overseeing and approving the development and implementation of a CSP, 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, as well as 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 should be composed of individuals from organizations, including security, operations, engineering, emergency preparedness, and other support organizations, as required, 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.

Pre-Decisional

An acceptable method for forming the CST is to include, assemble, or designate individuals who have expertise and experience 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. It includes knowledge of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant information systems. 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 plantwide and corporatewide networks.

- nuclear facility operations, engineering, and safety—This includes overall facility operations and plant technical specifications. The 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 should 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;

- reviewing and evaluating implementation of procurement procedures in accordance with the system and service acquisitions section (C.3.3.1);

- 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

Pre-Decisional

- ensuring 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 should have the authority to conduct an objective assessment, make determinations that are not constrained by operational goals (e.g., cost), implement the defense-in-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 A.3.1.2 of Appendix A provides a template that a licensee may use in describing the formation of its CST, and Section C.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, this document refers to licensee assets that are protected from cyber attack under 10 CFR 73.54 as CDAs. However, it may be difficult for a licensee to identify CDAs without first conducting a wider assessment of all the systems within the facility. A typical NPP contains hundreds of individual systems that contribute to the overall operation, safety, and security of the facility. Figure 3 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 public health and safety. Although all of these systems may not ultimately be within the scope of the licensee's cyber security program, the accurate identification of these plant systems associated with an 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, it can then use that information to establish the set of equipment that will be protected under its cyber security program. The following section describes one acceptable method to conduct this analysis.

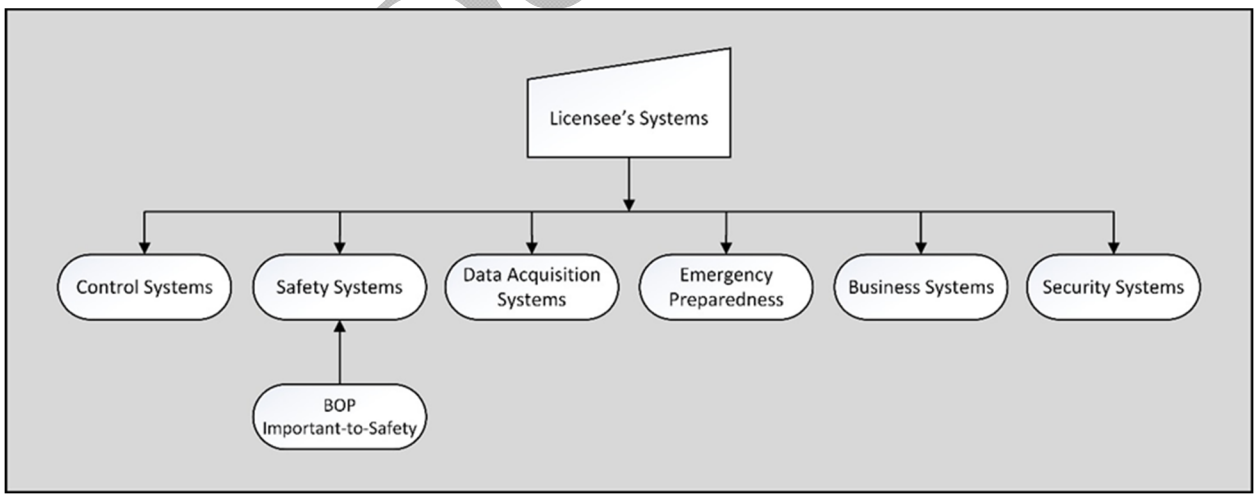

Figure 3 – Categorization of plant systems

To identify CDAs, a licensee should first identify the overall allocation and organization of plant systems, equipment, communication systems, and networks, including support systems, that are associated with the 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 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 that, 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 the "worst case" impact if the CDA were to be compromised.

For those support systems or equipment not directly associated with SSEP functions, the licensee should perform 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 are considered CSs.

In SRM-CMWCO-10-0001 (*See* Ref. 11), the Commission determined as a matter of policy that the NRC cyber security rule (10 CFR 73.54) should be interpreted to include SSCs in the BOP that have a nexus to radiological health and safety at NRC-licensed NPPs. The staff determined that such SSCs are those that could directly or indirectly affect the reactivity of an NPP. Therefore, they are within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1) and are included in the safety system section of Figure 3.

BOP systems that are subject to 10 CFR 73.54 are identified in a North American Electric Reliability Corporation survey known as the Bright-Line Survey. All NPPs were required to complete this survey by June 24, 2010 and maintain it as a matter of record (Ref. 28). This document should be reviewed to assist in identifying the physical and logical boundary for BOP SSCs (Ref. 29). The BOP SSCs that are beyond the first inter-tie with offsite power distribution systems are not considered to be within the scope of 10 CFR 73.54. All BOP SSCs within this inter-tie that meet the definition of a digital device should be assessed to determine whether they are a CDA (1) could directly or indirectly affect reactivity at an NPP and (2) could result in an unplanned reactor shutdown or transient and are therefore within the scope of the NRC's cyber security regulation.

The identification of CSs should include those systems, equipment, and devices that (1) perform or are relied upon for SSEP functions, (2) affect SSEP functions or affect CSs or CDAs that perform SSEP functions, (3) provide a pathway to a CS or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS or CDA, (5) protect any of the above from cyber attack up to and including the DBT, or (6) are BOP systems, equipment, and devices that affect reactivity and could result in an unplanned reactor shutdown or transient. Figure 4 illustrates this evaluation process.

Pre-Decisional

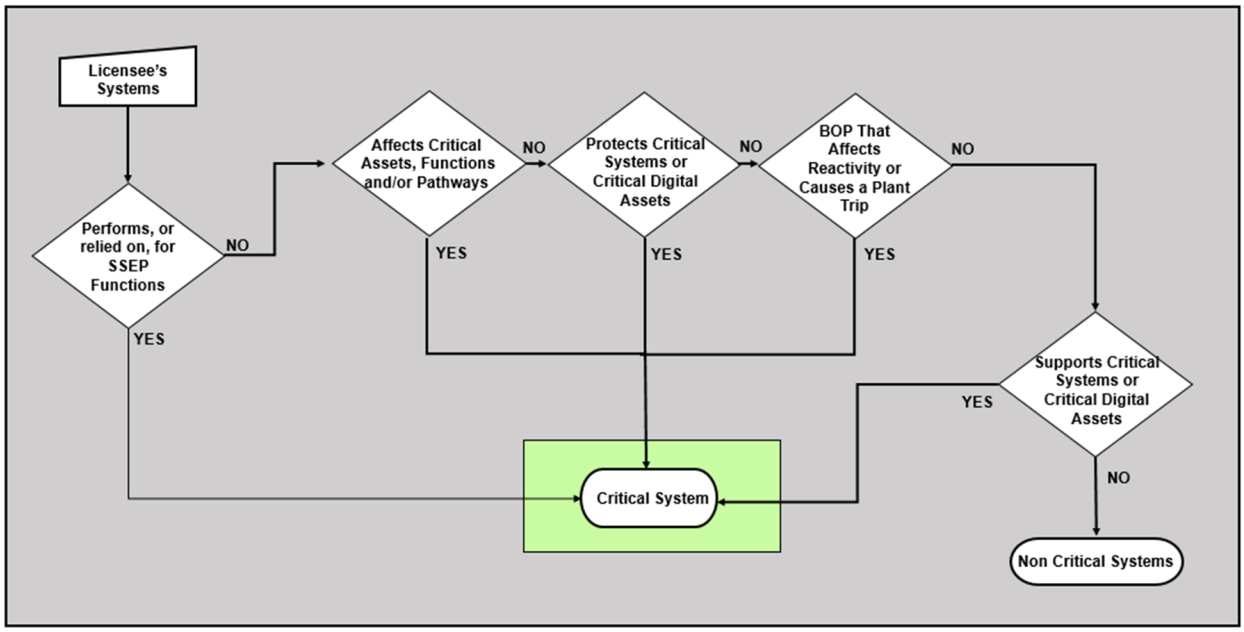

Figure 4 – Evaluation process for determining critical systems

Following identification of CSs, the licensee should 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 media, 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 meet one or more of the following criteria: (1) perform or are relied upon for SSEP functions, (2) could adversely affect SSEP functions or CSs or CDAs that perform SSEP functions, (3) provide a pathway to a CS or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS or CDA, (5) protect any of the above from a cyber attack, up to and including the DBT, or (6) are BOP equipment that affects reactivity and could result in an unplanned reactor shutdown or transient. Figure 5 illustrates the process of identifying CDAs. The NRC and NEI are working to revise NEI 10-04 to better identify CDAs within the scope of NRC's cybersecurity rule. However, the current version of NEI 10-04 has been found acceptable by the NRC for identifying CDAs associated with SSEP functions (Ref. 18).

Pre-Decisional

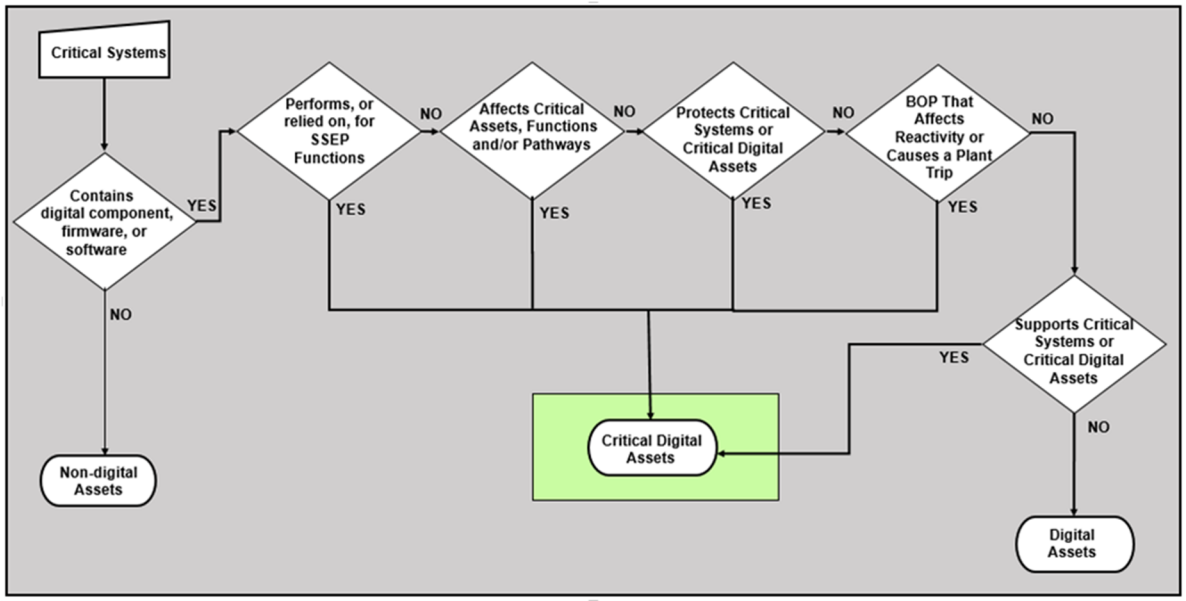

Figure 5 – Evaluation process for identifying CDAs

Digital computers, equipment, devices, communication systems, and networks that provide a pathway to CSs or CDAs that are associated with SSEP functions, are within the scope of the 10 CFR 73.54. This includes any support systems that are either directly or indirectly connected to systems that perform SSEP functions. For example, support systems and equipment may include, but are not limited to, digital maintenance and test equipment for CSs or CDAs that may not be permanently connected, but a cyber compromise of the support system and equipment could lead to an adverse impact on SSEP functions (e.g., maintenance laptop used to maintain, program, or diagnose a programmable logic controller). The licensee has the option of categorizing maintenance and test equipment as CDAs or as portable media and mobile devices (PMMD) (see Section B.1.19 of Appendix B).

A digital device that communicates to CSs and or CDAs need not be classified as a CDA simply because of the pathway, but these devices should be protected. A pathway, regardless of its underlying physical nature and basis, is also in scope for cyber security protection under the requirements in 10 CFR 73.54(a)(1) if the pathway within the protected digital computer and communication systems and an adversary can use networks to initiate a cyber attack on a CS or CDA. The pathway could exist between higher and lower security levels; between systems, devices, and CDAs on the same security level; or within a device (switches, multiplexers). The pathway can involve intervening systems, processes, and devices that aid in creating or maintaining the pathway. For a pathway to be excluded from the scope of inspection under 10 CFR 73.54, licensees must demonstrate that the associated attack vectors (delivery mechanism or vulnerability/exploit) do not exist by performing and documenting a comprehensive analysis of the pathway as specified in 10 CFR 73.54(b)(1).

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

Pre-Decisional

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 for a CDA or CS security assessment, the licensee should collect the following information:

- a general description of each system, asset, or network identified as a CS and CDA
- a brief description of the overall function provided by each CS and CDA
- 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 potential attack surfaces and attack pathways for each CDA
- 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 A.3.1.3 of Appendix A to this guide provides a template for licensees to use in preparing that section of the CSP that discusses the identification of CDAs.

C.3.1.4 Review and Validation

The objectives of the CDA assessment review are to evaluate 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 the licensee's 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

Pre-Decisional

The licensee can validate this information through a physical and electronic inspection of the system. The validation process should include 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 CSs and CDAs and trust relationships between the CSs and CDAs;

- 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 CSs and CDAs.

An electronic validation or scan is an acceptable way for licensees to validate the CDA assessment 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 are acceptable (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 A.3.1.4 of Appendix A to this document provides a template for licensees to use in preparing the section of the CSP that 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 integrated defense-in-depth protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks. An acceptable defense-in-depth protective strategy comprises the following elements:

- a defensive architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation within each security level, and

- a defensive strategy that employs multiple, diverse, and mutually-supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyber attack.

Pre-Decisional

To comply with this requirement, licensees should implement 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.

From a defensive architecture perspective, defense-in-depth involves setting up multiple security boundaries to protect CDAs and networks from a cyber attack. In this way, multiple protection levels of mechanisms must fail for a cyber attack to progress and impact a CS or network. Defense-in-depth defensive strategies are represented by documented collections of complementary and redundant security controls that establish multiple layers of protection to safeguard CDAs. Under a defense-in-depth defensive 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.

For example, while a data diode can be an important element of an acceptable defensive architecture, use of a data diode alone does not provide adequate protection to comply with the defense-in-depth strategies required by 10 CFR 73.54(c)(1). Exploits of vulnerabilities associated with supply chain, PMMD, wireless, and physical presence pathways can allow an attacker to circumvent the protection provided by the data diode implementation. Additionally, if a violation of policy or if protection mechanisms were bypassed (e.g., by a new virus that is not yet identified as a cyber attack), the use of a data diode would not provide protection. However, implementing defense-in-depth strategies (use of a data diode with the application of the security controls in Appendices B and C in accordance with Section C.3.3 of this guide) would mean that mechanisms would still be 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 receiving an adverse impact. This is an example of an adequate implementation of protection that complies with the defense-in-depth protective strategies.

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 to, prevent, detect, and mitigate an attack on a CDA and assist with recovery.

C.3.2.1 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 that 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 6 shows 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 the most secure level of the defensive architecture. When one-way communication is required in the defensive architecture, hardware characteristics that enforce unidirectional communication feature(s) (e.g., the use of a unidirectional/nonsoftware-based link that is connected to a transmitter in the higher security level and a receiver in the lower security level) are the preferred means of implementation. The logical model shown below does not always correspond directly with the physical locations such as the vital, protected, or owner-controlled areas. The following concepts apply to systems associated with SSEP functions:

Pre-Decisional

- Functions are protected commensurate with their safety and security significance through the determination and use of appropriate security levels. The security level defines the degree of security needed to protect the function, based on the consequences to plant safety and security from loss or impairment of the function due to cyber attacks. This is an example of a consequence-based, graded approach for risk-informed security.

- Each function is implemented by one or more critical systems. A system's allocation to a security level is determined by its associated function with the highest safety or security significance.

- Protection of the function depends on the proper implementation of technical and nontechnical cyber security requirements for the security level. Proper implementation of these requirements is dependent upon understanding the attack surfaces and environments associated with the technologies used within a CS or CDA.

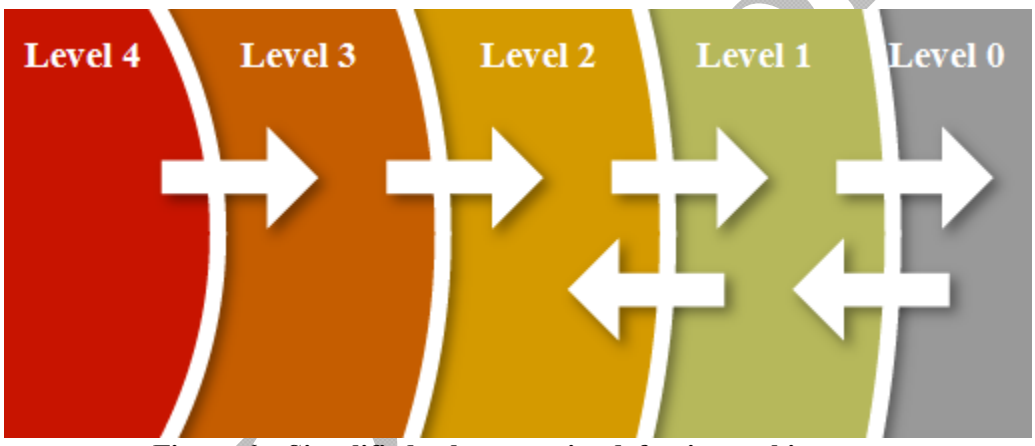

Figure 6 – Simplified cyber security defensive architecture

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 that, 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.

- It ensures that data flow from one level to other levels occurs through a device that enforces the security policy between levels and can detect, prevent, delay, mitigate, and recover from a cyber attack coming from the lower security level.

- Initiation of communications from digital assets at lower security levels to CDAs at higher security levels should be implemented on a "deny-all, permit-by-exception" basis, and the exceptions should be supported by a complete justification and security risk analysis.

- Data only flow from one level to other levels through a device or devices that enforce security policy between each level.

Pre-Decisional

- It 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.

- Implementation of the multiple, diverse technologies used within the plants addresses the attack surfaces and environments associated with the technologies so that the protections of the defensive architecture are not bypassed or circumvented.

- CDAs and boundary protection systems are configured as described in Section B.5 of Appendix B and Section C.7 of Appendix C.

For this defensive architecture to be effective in protecting CDAs from cyber attacks, the licensee should consistently apply 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 it should adopt the security controls identified in Section C.3.3 of this guide. All CDAs should be protected commensurate with their security and safety significance. As discussed in Section C.3.3, the licensee may implement a graded approach built on a consequence-based analysis that aims at defending the plant safety against cyber threats.

While the defense architecture may allow communications between systems within the same level (e.g., Level 4 or Level 3), the digital isolation of CDAs (i.e., no digital communication pathways between a CDA and any other digital asset) is a mechanism to meet many of the requirements specified in 10 CFR 73.54. Incorporating analog communication at strategic points within the defensive architecture is one example of digital isolation implementation.

Section A.3.1.5 of Appendix A to this guide includes a template for licensees to use in preparing the section of the CSP on using 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 power reactors' SSEP functions and cause high negative impact to public health and safety. Thus, to provide high assurance that CDAs are protected from cyber attacks, known potential cyber risks to these CDAs must be addressed. One way to do this is 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 power reactor.

The purpose of any given security control is to achieve one or more of the following objectives:

- mitigating vulnerabilities (e.g., patching software or training personnel on social engineering)

- mitigating the consequences of an attack (e.g., encrypting sensitive information or using diverse backup systems)

- defending or blocking an attack vector (e.g., installing a firewall between local area network segments or having user accounts with passwords)

Pre-Decisional

- detecting an attack (e.g., installing an intrusion detection system on a network or installing antivirus scanning on a personal computer)

- recovering from an attack (e.g., having backup and restoration files for CDAs or incident response training and exercises)

- assessing the security posture of a device (e.g., performing a vulnerability scan on a CDA)

- protecting the confidentiality, integrity, and availability of information (e.g., encrypting message traffic or generating backups)

- evaluating the effectiveness of the overall cyber security program and the controls implemented in the context of the current threat environment (e.g., review patch releases or threat notifications)

- ensuring that the plant CDAs have adequate overall cyber security and that the required defense-in-depth is established and maintained (e.g., through specialized cyber security training or formation of the CST)

The concept of a defense-in-depth defensive strategy is that multiple layers of defensive security controls are placed throughout the system with the intent of providing overlapping defenses in the event that a control fails, or a vulnerability is exploited. Therefore, each implemented security control can serve an additional purpose of contributing another defensive control to the defense-in-depth security architecture.

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.

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 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 cannot be implemented, use alternative controls or countermeasures that provide at least an equivalent level of protection against the threat or attack vectors and vulnerabilities or weaknesses associated with one or more of the security controls enumerated in Appendix B by accomplishing the following:

    - 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, and

    - implementing alternative countermeasures that provide at least the same degree of protection as the corresponding security control in Appendix B.

Pre-Decisional

- 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.

- Apply the security controls described in Appendices B and C to this guide, based on the maximum consequences of a successful cyber attack on the CDAs in terms of plant safety and security.

The analysis done in support of this consequence-based, graded approach should be rigorous and repeatable by ensuring reproducibility and consistency of the applied security controls posture. The NRC and NEI are working to revise NEI 13-10 to better apply security controls for the protection of CDAs within the scope of NRC's cybersecurity rule. However, the current version of NEI 13-10 Revision 6 (Ref. 20), documents an acceptable approach for applying security controls using a consequence-based, graded approach.

A review by a licensee of all cyber security controls in determining each control's applicability for mitigating cyber risks for a CDA, a group of CDAs, or a CS can be described as a top-down approach. Using this approach, a licensee would provide documented justification demonstrating why a given cyber security control(s) was not implemented. Licensee analysis and assessments that provide documented justification demonstrating why a set of security controls is applied to a CDA, a group of CDAs, or a CS to mitigate cyber risks can be described as a bottom-up approach. Both risk-informed approaches are technically acceptable and rely on comprehensive assessments of the attack surface and consequence analyses to support claims of adequate protection of a CDA, a group of CDAs, or a CS.

Common controls and inherited controls are both potentially acceptable as alternate countermeasures as long as it can be documented and demonstrated that they mitigate the threat vector the control is intended to protect against and would not decrease the effectiveness of the security control.

If multiple CDAs share the same features, options, or functions regardless of their specific process applications, it may be acceptable for the licensee to perform a single comprehensive analysis on a selected sample device or CDA and apply that analysis to every other instance of the same device throughout the plant. This analysis includes determining which security controls will be applied, considering common, inherited, or alternative controls for every instance of that particular CDA or device. The following CDA characteristics are among those that should be considered when grouping CDAs:

- configuration baseline (CDAs configured using the same approved baseline configuration)
- operation (CDAs operated in the same manner)
- function (CDAs performing the same functions)
- operating environment (CDAs operated in the same manner, in the same environment)
- location (owner-controlled area, protected area, vital area)
- maintenance (CDAs maintained in the same manner)

NEI 13-10 guidance for protecting CDAs for safety, important to safety, BOP, and emergency preparedness provide examples of grouping CDAs by functions.

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 effect, the licensee should use alternate controls to protect the CDA from a cyber attack up to and including the DBT, consistent with the

Pre-Decisional

process for selecting alternate controls as described above. Any residual vulnerability in a CDA should be mitigated or, if possible, eliminated by alternate controls if a security control is not used because of concern over its impact on the CDA's function.

Once the security controls have been implemented, the CST would conduct both an effectiveness analysis, as described in Section 4.1.2, and vulnerability assessments or 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 Appendices B and C.

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

C.3.3.1 Technical Security Controls

Technical security controls are safeguards or protective measures that are executed through automated 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 security controls, actions are preplanned or preprogrammed and automatically executed in response to a triggering event or are configured to provide electronic enforcement of policy. These actions generally do not require human intervention. Applicants for design certification may incorporate technical security controls as part of the nuclear power reactor design. Sections C.3.3.1.1 through C.3.3.1.5 of this guide describe acceptable methods to implement technical security controls.

C.3.3.1.1 Access Control

Access control ensures that only authorized personnel are granted physical or logical access to CSs, networks, and CDAs.

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
- documented 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)

Pre-Decisional

- 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 B.1 of Appendix B to this guide

C.3.3.1.2 Audit and Accountability

Audit and accountability ensure that sufficient controls are in place to provide auditable evidence to account for, respond to, and minimize the impact of incidents that can affect CDAs. They help accomplish several security-related objectives, including but not limited to, individual accountability, reconstruction of events (actions affecting a CDA), incident detection, and problem analysis.

Audit and accountability include 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

- documented procedures to facilitate and maintain audit and accountability policy

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

C.3.3.1.3 System and Communications Protection

System and communications protection ensures that communication flows within and among CDAs, CSs, and networks are properly configured; secure from unauthorized modification or eavesdropping; and properly partitioned and segregated, and that the systems, networks, and information flows are free from outside or unauthorized influence.

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

- documented procedures to facilitate and maintain system and communications protection policy and associated system and communications protection controls

- implementation of the security controls described in Section B.3 of Appendix B to this guide

C.3.3.1.4 Identification and Authentication

Identification and authentication mechanisms give a digital device or system a means of determining and verifying the identity of a user or a process accessing a CDA. By using these mechanisms, the user or process can be associated with applicable system permissions and constraints (i.e., access control).

Pre-Decisional

Identification and authentication protection includes the following elements:

- management of user identifiers by the following methods:
  - uniquely identifying each user or application acting as a user
  - verifying the identity of each user or 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 the 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 documented 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 B.4 of Appendix B to this guide

C.3.3.1.5 System Hardening

System hardening involves configuring a CDA to provide only essential functions. The determination of the essential functions should take place during the CDA security assessment, and the documented CDA security assessments should reflect the system hardening measures. Benefits provided by system hardening include, but are not limited to, the following:

- a smaller attack surface, which can reduce the number of security controls needed to eliminate vulnerabilities
- a reduction in the amount of data to be monitored and analyzed by the licensee to determine the security posture of the protected asset or system

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
- documented procedures to facilitate and maintain system hardening policy
- implementation of the security controls described in Section B.5 of Appendix B to this guide

C.3.3.2 Operational Security Controls

Pre-Decisional

Operational security 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 security 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 security 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
- documented procedures to facilitate and maintain the media protection policy
- implementation of the security controls described in Section C.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
- documented procedures to facilitate the implementation of the personnel security policy
- implementation of the security controls described in Section C.2 of Appendix C to this guide

C.3.3.2.3 System and Information Integrity

System and information integrity include 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
- documented procedures to facilitate and maintain the system and information integrity policy
- implementation of the security controls described in Section C.3 of Appendix C to this guide

C.3.3.2.4 Maintenance

Maintenance includes the following elements:

Pre-Decisional

- a written policy that defines the purpose, scope, roles, responsibilities, and management commitments associated with performing routine and preventive 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

- documented procedures to facilitate and maintain the maintenance policy

- implementation of the security controls described in Section C.4 of Appendix C to this guide

C.3.3.2.5 Physical Protection

Physical 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 mitigation of the risk of unauthorized physical access to CDAs and associated communication pathways

- documented procedures to facilitate and maintain physical protection policy

- implementation of the security controls described in Section C.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 programs 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. Furthermore, consistent with requirements stated in 10 CFR 73.54(d)(4), the licensee must make cyber security event notifications in accordance with the provisions of 10 CFR 73.77. A cyber security event must be reported within the timeframe specified in 10 CFR 73.77(a). In addition, consistent with the requirements stated in 10 CFR 73.54(e)(2), the CSP (and therefore the cyber security program) must include incident response and recovery measures by describing how to accomplish the following:

- maintain the capability for prompt 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 address 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 documented procedures to facilitate the implementation of incident response policy and associated incident response measures;

- develop documented procedures to facilitate the implementation of the incident response investigations, based on the guidance found in the following:

Pre-Decisional

- NIST SP 800-61, "Computer Security Incident Handling Guide," Revision 2, issued August 2012 (Ref. 30)
- NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," issued August 2006 (Ref. 31)
- DHS Cybersecurity and Infrastructure Security Agency, "Cyber Resiliency Review Implementation Guide, Volume 5: Incident Management," issued 2016 (Ref. 32) and

- implement the security controls described in Section C.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 designs 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 address 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 C.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 address 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 a 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 to take measures to correct the deficiency

Pre-Decisional

- develop, disseminate, and periodically review and update procedures to facilitate and maintain the security training and awareness program

- implement the security controls, as described in Section C.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, evaluates 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 address the following elements:

- develop, disseminate, and annually review and update the configuration management policy and program that define the purpose of the nuclear facility's configuration management policy, scope, roles, requirements, responsibilities, and management commitments necessary to determine with high assurance that a modification to a CDA does not reduce the existing security and that 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 documented 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 C.11 of Appendix C to this guide.

C.3.3.3 Management Security Controls

Management security controls are those controls 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 security controls.

C.3.3.3.1 System and Service Acquisition

An acceptable approach to system and service acquisition should include 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 documented procedures to facilitate and maintain the implementation of procurement policies associated with vendor security and development life cycles

- implementation of the security controls described in Section C.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. 3 (see Ref. 8).

Pre-Decisional

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 ensures that cyber security risks are appropriately evaluated and managed. 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 A.4 of Appendix A to this guide, and Section C.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 incorporates 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. An effective integration process should consider, but is not limited to, the following elements:

- 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 the 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 on the needs of both disciplines; and
- periodically exercising the entire security force using multiple realistic scenarios combining both physical and cyber simulated attacks.

Pre-Decisional

Section A.3.2 of Appendix A to this guide contains a template for the licensee to use in preparing the section of the CSP 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 does not need to submit these policies, implementing procedures, site-specific analyses, or other supporting technical information of the CSP to the NRC for prior review and approval. However, such information must be available for inspection by the NRC staff. The cyber security program should include documented 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 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 procedure 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 of this guide

C.4 Maintaining the Cyber Security Program

Once the cyber security program is in place, 10 CFR 73.54(d)(2) requires licensees to "evaluate and manage cyber risk." One acceptable method for evaluating and managing cyber risk 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 program effectiveness;
- vulnerability scans and assessments;
- change control; and
- security program review.

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

Pre-Decisional

C.4.1 Continuous Monitoring and Assessment

Continuous monitoring and assessment ensures that 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 in the system, network, environment, or emerging threats does not diminish the effectiveness of these controls, processes, or procedures.

Continuous monitoring includes the following:

- ongoing assessments to verify that the security controls implemented for each CDA remain in place throughout the life cycle;
- ongoing verification that rogue assets are not connected to the infrastructure;
- continuous monitoring of inbound and outbound network traffic and analysis of event logs;
- ongoing assessments of the need for and effectiveness of the security controls identified in Appendices B and C to this guide;
- periodic vulnerability scans and assessments;
- ongoing verification using established baseline configurations that CDAs are being protected commensurate with their safety and security significance; and
- periodic cyber security program reviews to evaluate and improve the effectiveness of the security program.

It is important for licensees to understand normal and expected behavior of digital assets in order to monitor for and detect abnormal behavior. System manufacturers and suppliers may be the best sources for this information and this information should be captured in the Licensee's security assessment for each device. Firewalls can be configured to deny all communication except for finely tuned expected behavior and use of communication protocols. The licensee should understand the minimum functionality needed on a device to execute the required functions at the plant. This knowledge will facilitate minimizing the attack surface through implementation of least functionality and system hardening security controls on the devices. These actions will support anomaly detection by a HIDS, NIDS, or SIEM.

Continuous monitoring may require updates to the CSP to reflect changes necessary to maintain high assurance that CDAs are adequately protected from cyber attacks. Section A.4.1 of Appendix A to this guide provides a template for licensees to use when preparing the CSP to ensure the effective 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 such 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 A.4.1.1 of Appendix A to this guide contains a template for licensees to use in describing the ongoing assessment process for security controls in the CSP.

Pre-Decisional

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. Fully understanding the pathways (i.e., direct and indirect connections) among digital assets—including interconnections through security devices (e.g., data diode, firewalls)—will facilitate the licensee's evaluation of the security controls' effectiveness. The licensee should verify the effectiveness of security controls when they are initially applied to a CDA to establish a baseline and subsequently verify them periodically, 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; reevaluation of 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 on the efficiency of the periodic maintenance and life cycle support activities.

Effectiveness and efficiency are measures of two aspects of security control implementation:

- the robustness of the security control, referred to as effectiveness; and
- the timeliness of the result that the control is designed to produce, referred to as efficiency.

Based on this information, the licensee should conduct an effectiveness analysis to identify areas of improvement in the cyber security program. This effectiveness analysis should provide key information about the results of previous policy and acquisition decisions. It should also do the following:

- 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 A.4.1.2 of Appendix A to this guide includes a template for the licensee to use in preparing the CSP on implementation of the effectiveness analysis of security controls.

Various security controls in Appendices B and C of this guide identify the use of reviews, assessments, and audits. The data collected from these processes are useful as metrics in the analysis of security controls by accomplishing the following:

- helping determine the effectiveness of implemented security processes, procedures, and controls;
- aiding in identifying specific security controls that are implemented incorrectly, not implemented, or ineffective;

Pre-Decisional

- serving as an important part of the detection and program improvement process; and

- providing a quantifiable "scoring system," which can be useful in advancing the security goals and objectives and implementing the CSP.

These metrics, along with the analysis of security controls, can also be used to support the following security program activities in 10 CFR 73.55:

- security program reviews, and

- maintenance, testing, and calibration.

Regulations under 10 CFR 73.55(m) require security program reviews for each element of the physical protection program. Maintenance, testing, and calibration ensure that systems and equipment are tested for operability and are capable of performing their intended functions in accordance with 10 CFR 73.55(n).

The selection of metrics for analysis is an iterative process, which includes reviewing and assessing the outcomes of prior analyses and refining the metrics used for future analyses. As a licensee's cyber security program matures, the quantity and quality of data that can be used for effectiveness analysis will likely become increasingly refined and mature. It is possible for licensees to provide evidence of the effectiveness of their cyber security program without implementing cyber security metrics, and therefore, this guidance is presented as an option. However, establishing a metrics program has the advantage of being less intrusive to a system than penetration or vulnerability testing, can require fewer resources than some manual assessments, and builds on many activities required by most CSPs. Additionally, establishing and maintaining metrics will provide a mechanism to tie the data obtained from cyber security program activities to cyber security control implementation.

The following is one acceptable method for selecting and maintaining cyber security metrics:

(Step 1) Define measurement goals and objectives as related to the security goals of 10 CFR 73.54.

A licensee's CSP typically includes assessments, reviews, and audits. Performing this step will facilitate a mechanism for the licensee to link the implementation of these metric generating activities to security objectives. Here is an example of a security goal and several security objectives:

- Goal—Establish effective analyses of metrics that allow for the continuous improvement of the cyber security program.

- Objective 1—Generate metrics that demonstrate, within the scope of the cybersecurity program, that the CSP implementation protects plant computers and digital equipment from malware.

- Objective 2—Generate metrics that demonstrate the CSP implementation protects the availability and integrity of data and software on plant computers and digital equipment.

- Objective 3—Generate metrics that demonstrate the CSP implementation establishes and maintains effective cyber security training for facility personnel.

- Objective 4—Generate metrics that demonstrate the CSP implementation establishes and maintains an effective incident response and recovery plan for cyber attacks.

Pre-Decisional

- Objective 5—Generate metrics that demonstrate the licensee continuously evaluates and manages cyber risks.

- Objective 6—Generate metrics that demonstrate modification to an asset does not adversely affect the system.

This methodology also supports the definition of lower level objectives that link to the higher level objectives. As an example, lower level objectives for objective 1 (malware protection) could be defined based on the SSEP functions protected from malware. As security controls are applied to digital assets and critical systems, the protections afforded by the controls will protect the SSEP functions. Generated metrics should provide evidence of the malware protection for SSEP functions.

(Step 2) Define what metrics to capture and track to best measure the effectiveness of the CSP (reevaluate and, if necessary, change over time as program matures).

The generation of metrics is not an end in itself. Rather, metrics should be selected and tailored according to the objectives of the analysis. The metrics should support one or more of the objectives listed in step (1). Actions in this step should define *what* should be measured to provide a useful metric. The metrics produced in this step should be a list of auditable events (see Section B.2.2 of Appendix B to this guide). This step of a cyber security metric program can support defense-in-depth protective strategies by linking metrics from multiple overlapping and complementary security controls to measure the effectiveness of a single security objective. Examples of metrics to support objective 1 (protecting CDAs from malware) are listed here. Note that a single metric can support multiple security objectives.

- administrative
    - number of training or procedure deficiencies related to the cyber security program
- access control (CDA/CS)
    - number of violations of PMMD
    - flaw remediation,
        - mean time to patch
        - number of failures or issues post-patching
        - number not patched
- malicious code identification
    - number of incidents identified at the appropriate point of detection
    - number of incidents not identified at the appropriate point of detection
- security functionality
    - number of failures or degradations of security functionality
    - mean time to respond
    - mean time to repair/replace or take compensatory measures
- security alerts and advisories
    - average time to evaluate

Pre-Decisional

- average time to respond (implementation of protective measure)
- number of critical vulnerabilities for each CDA or CS

- software and information integrity

  - number of unauthorized changes or attempted changes
  - number of software integrity verification failures
  - number of violations of whitelisted services or processes executed or execution attempted

- miscellaneous

  - false positives (e.g., host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), antivirus)

  - repeat items or findings from vulnerability scans

(Step 3) Develop strategies for generating and capturing metrics (e.g., log files, audit records).

Actions in this step should define *how* to capture the data to provide a useful metric that was identified in step (2). The data generated and captured in this step can be based on implementation of RG 5.71 technical security control B.2.3 (content of audit records) and B.2.12 (audit generation) in Appendix B to this guide. Data in this step may also rely on configuration management data (i.e., operation and maintenance security control C.11.9 (component inventory) in Appendix C to this guide) and any security controls involving event monitoring or reporting. Examples of strategies for generating and capturing metrics include the following:

- develop documented policy and procedures for reporting and tracking cyber security incidents (e.g., training and procedure deficiencies, infractions)

- generate and audit logs using HIDS or other technologies on CDAs

- extract CDA log information and work records for patch updates on CDAs

- extract and audit log information from firewalls, gateways, PMMD kiosks, antivirus software applications, and log files on signature updates

- log instances of security functionality verification failures on CDAs and extract logs for analysis

- review the following:

  - Industrial Control Systems Cyber Emergency Response Team and other credible sources for vulnerability updates

  - hardware and software vendors for critical vulnerabilities identified and patches and updates available

  - extracted log files for software integrity failures (e.g., checksum failures, digital signature verification failures) from PMMD and kiosks, software integrity verification software on CDAs, and CDA hardware tamper reports

Pre-Decisional

It is critical for the licensee to make some determination about the scope of coverage for the implemented metrics. If metrics are generated for only a percentage of devices, this information must be considered when analyzing and reporting the resulting data.

(Step 4) Establish benchmarks and targets for metrics captured and tracked.

The licensee should set performance targets that are consistent with the goals and objectives listed in step (1) that the licensee wants to achieve. These targets should be specific, measurable, achievable, realistic, and time-targeted (SMART). Performance targets, based on metrics defined in step (3), should be justifiable and quantitative with measurable outcomes. Some examples of performance targets are as follows:

- the number of personnel that received cyber security awareness training versus the total number of employees
    - performance goal: documentation that all the employees received qualified cyber security training
    - actual metric: number of employees who passed a qualified cyber training course versus total employees
- the number of incidents not identified at the appropriate point of detection
    - performance goal: zero incidents of unauthorized communication between CDAs on Level 3 or 4
    - actual metric: the number of unauthorized communication attempts logged by a HIDS on Level 3 or 4
    - performance goal: zero incidents of malware detection on Level 3 or 4 CDAs
    - actual metric: the number of incidents of malware detection on Level 3 or 4 CDAs

(Step 5) Establish a formal reporting/review/refinement cycle.

A metrics reporting process is needed to describe how the data will be collected and formatted for analysis and presentation, when and how often the data will be collected (event driven, periodic), and who will collect the data (people, automated tool). This step should also result in continual improvement of the cyber security metrics. Continual improvement activities can include, but are not limited to, the following:

- soliciting feedback from key stakeholders;
- revising collection and analysis techniques, based on lessons learned and other feedback;
- revising implementation procedures; and
- refining cyber security benchmarking data.

RG 5.71 technical security control B.2.6 (audit review, analysis, and reporting) is implemented during this step. Based on the analysis of the metrics, decisions to revisit earlier steps of this process may occur.

C.4.1.3 Vulnerability Scans and Assessments

Pre-Decisional

Vulnerability assessments and scans can reveal security vulnerabilities in a plant's digital infrastructure. These vulnerabilities within a plant's digital infrastructure design or implementation have the potential to degrade the plant's safety or security posture if the vulnerabilities are not properly mitigated. Without the use of vulnerability assessments and scans of digital assets, licensees cannot effectively understand the possible impact of a cyber security incident. Vulnerability scans and assessments identify security deficiencies in CDAs. Licensees should conduct periodic vulnerability assessments or scanning of all CDAs, when specified by the security controls described in Appendices B and C to this guide, and when new vulnerabilities that could affect the security posture of CDAs are identified. Often overlooked devices such as scanners, copiers, and printers that are connected to CDAs or operate on the same network as the CDAs should also be scanned for vulnerable versions of software, improper configuration, and unnecessary or nonsecure functions, ports, protocols, and services. These overlooked devices often have functions, ports, protocols, and services that are not needed or contain firmware that is not kept up to date, and thus they are vulnerable to compromise. Once compromised, the attackers can use these devices as staging points for collecting sensitive information, to set up a persistent presence for later attacks against other CDAs, or to penetrate deeper into the defensive architecture.

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 or virtualize) before scanning. Section A.4.1.3 of Appendix A to this guide includes a template for licensees to use in preparing the CSP for 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, licensees should (1) implement Section A.4.2 of Appendix A and the security controls in Section C.11 of Appendix C, and then (2) establish, maintain, and document a baseline configuration of the CDAs. This baseline should include, 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 or hardware components.

The documentation necessary for effective change management includes, but is not limited to, a log of configuration changes that 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 recommendations on change control.

Pre-Decisional

C.4.2.1 Configuration Management

Configuration management ensures that the site's cyber security program objectives remain satisfied by controlling the addition of new CDAs and the changes made to CDAs throughout their life cycles. During the operation and maintenance phases of the CDA life cycle, effective configuration management ensures that the addition of new CDAs or 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 promptly and effectively implement each of the controls specified in Appendices B and C to this guide. The reimplementation of controls and any configuration changes can change the security assessment of a CDA. The licensee should ensure that it documents any modification to the CDA in its assessment. This will ensure that security controls are still properly addressed after a configuration management change and that the security assessment reflects an accurate, current view of the CDA's security posture. 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 the addition of CDAs or modifications to CDAs before their implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained. Section A.4.2.1 of Appendix A to this guide includes a template that licensees may use 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., because of 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 of Changes and Environment

The security impact analysis assists in managing potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats. Sections C.3.5, C.10.9, and C.12.4 of Appendix C to this guide describe mechanisms to monitor emerging threats. Section A.4.2.2 of Appendix A to this guide includes a template that licensees may use to conduct 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 the 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.

Pre-Decisional

Licensees should conduct 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 should implement the new security controls, as described in Section 4.2.2, to mitigate any gaps identified in the analysis. After the evaluation and implementation of controls, the licensee should ensure that it documents any changes impacting a CDA in or associated with the CDA's security assessment.

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

C.4.3 Cyber Security Program Review

In accordance with 10 CFR 73.54(g), the licensee reviews 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 a 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; and

- develop and implement documented procedures to facilitate and maintain the review program.

Licensees should complete a program review at least every 24 months. In addition, licensees should conduct the following 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; and

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

To meet the requirements of 10 CFR 73.55(m)(3), the licensee must document the results and recommendations of the program reviews, management's findings on 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 A.4.3 of Appendix A to this guide includes a template that licensees may use in documenting this process in a CSP.

Pre-Decisional

C.5 Records Retention and Handling

In accordance with 10 CFR 73.54(h), the licensee retains all records and supporting technical documentation 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 can 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 CSP. 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 A.5 of Appendix A to this guide includes a template for the licensee to use in preparing the CSP for records retention and handling of security controls.

Pre-Decisional

D. IMPLEMENTATION

The NRC staff may use this regulatory guide as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this regulatory guide to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," (Ref. 33), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

Pre-Decisional

GLOSSARY

access control The control of entry or use, to all or part, of any physical, functional, or logical component of a critical digital asset (CDA).

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

adverse impact A direct deleterious effect on safety, important-to-safety, security, or emergency preparedness functions; or the operation of systems, networks, and associated equipment; or the integrity and confidentiality of data and software. Examples include 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; or the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency. If 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 defined by 10 CFR 73.54(a)(2).

air gap An interface between two systems at which (1) they are not connected physically and (2) any logical connection is not automated—any data are transferred through the interface only manually, under human control (e.g., computers containing safeguards information where all digital assets are part of the same network and there is no communication outside the network).

assessment The testing or evaluation of policies, procedures, or controls to determine the extent to which the policies, procedures, or controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the cyber security requirements.

attack pathway Pathway (including physical access, wired connectivity or communications, wireless connectivity or communications, supply chain, or portable media and mobile devices) used or that may be used to gain access to a digital asset.

attack surface The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.

attack vector Means, method, mechanism, or technique (or combination thereof) used or might be used by an adversary to gain unauthorized access to, exploit a vulnerability in, produce a malicious outcome on, or otherwise cause adverse impact to a digital asset, network, or system.

Pre-Decisional

authentication	Verifying the identity of a user, process, device, or application acting as a user or verifying the origin of 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."
automated	An assembly of computer hardware, software, and firmware that is configured to collect, create, communicate, compute, disseminate, process, store, or control data, information, hardware, or plant equipment.
balance of plant (BOP)	The remaining systems, components, and structures that comprise a complete nuclear power plant and are not included in the nuclear steam supply system. (Source: 10 CFR 170.3, "Definitions")
bidirectional communications	Transmission and receipt of data or signals between devices occurring in either direction along a communications medium. Transmission Control Protocol 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 CDAs, systems, or networks contained within adjacent defensive levels.
bright line	The jurisdictional delineation of nuclear power plant systems, structures, and components between NRC regulatory oversight and that of the Federal Energy Regulatory Commission.
commercial off-the-shelf	Software or hardware products that are ready made and available for sale to the general public.
compromise	A change to the state of a hardware, software, or firmware asset such that it performs outside of the intended functionality due to a loss of confidentiality, integrity, or availability of data, configuration, settings or system function; alteration of existing functionality; or introduction of new functionality.
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 (Ref. 34))
countermeasure	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information or automation system. Actions, devices, procedures, or techniques that meet or oppose a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. Synonymous with security controls and safeguards.
credible	Describes information received from a source that has been determined to be reliable (e.g., law enforcement, government agency, US CERT) or that has been verified to be true. A threat or vulnerability can be verified to be

Pre-Decisional

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.

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

critical system 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 An individual who guards and protects or maintains, especially one entrusted with guarding and maintaining property or records.

cyber attack Any event in which there is reason to believe that an adversary has committed or caused, or has attempted to commit or cause, an adverse impact on a safety-related, security, or emergency preparedness function.

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 level.

digital device A device that stores, processes, or transmits data in a digital (as opposed to an analog) form.

external systems Systems that are outside the control of a licensee or applicant such that the licensee or applicant has no direct supervision or authority over the application of security controls or the assessment of the security controls. External systems include, but are not limited to (1) personally owned information systems or devices (e.g., notebook computers, smart phones, tablets, personal digital assistants), (2) privately owned computing and communications devices resident in commercial or public facilities, (3) systems owned or controlled by other organizations, (4) systems that are not owned by, operated by, or under the direct supervision and authority of the licensee or applicant, and (5) cloud service providers (e.g., infrastructure as a service, platform as a service, or software as a service).

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) or operating system call profiles.

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

Pre-Decisional

indicators of potential attacks	Early warnings revealing suspicious and anomalous events or behaviors. These include, but are not limited to, unusual account behaviors, atypical network patterns, login irregularities and failures, spikes in database read volumes, unexplained configuration changes, and anomalous files on CDAs. By identifying these indicators of potential attacks early, a licensee can potentially interrupt or prevent a compromise instead of responding to one.
information at rest	The state of information when it is located on storage devices as specific components of, or associated with, critical systems or CDAs, or both.
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	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	An intrusion detection system that has the ability to take actions to preempt or stop activities identified as malicious.
malware	Malicious software designed for infiltrating or damaging a digital device, without the licensee's or applicant's consent; software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system or function; or a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
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.
mobile device	Any nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, processing, or transmitting data, video or photo images, or voice emanations. This definition generally includes, but is not limited to, laptops, personal digital assistants, pocket personal computers, palmtops, media players (MP3s), memory sticks (thumb drives), cellular telephones, personal electronic devices with cellular phone capability, and pagers.

Pre-Decisional

network Group of components that share information or interact with each other to perform a function.

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

pathway The route or channel that can be used to achieve a result, including access to an asset, network, or system. A pathway can involve intervening systems and processes, as well as devices that aid in creating or maintaining the pathway. Pathways include, but are not limited to, wired (local area or wide area network) connectivity, wireless connectivity, serial (wired or wireless) communications, physical access, supply chain, and portable media and devices.

portable media A readily transportable single-purpose item that is exclusively designed for the digital storage of data and has the capability of transferring data from one information system to another. Examples include floppy disks, CD/DVDs, flash memory cards, and the data container portion of thumb drives and external hard drives.

Notes: At a minimum, all C.1 media protection controls apply to portable media. Many devices have storage capability but include electronics and have extended functionalities beyond the storage of data. These devices are more appropriately defined as mobile devices (e.g., memory sticks, portable media players, cell phones, laptops, tablets, digital cameras, external hard drives, media servers). Mobile devices must be analyzed to determine the appropriate controls (e.g., Section B.1.19 of Appendix B).

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 an 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 CDA, computer, or node that is physically located in a less secure defensive level.

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

security control A safeguard or countermeasure prescribed for a device, system, or organization designed to protect the confidentiality, integrity, and availability of its information and function and to meet a set of defined security requirements.

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.

Pre-Decisional

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 that, if compromised, 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 that 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 that, if compromised, 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 that, if compromised, could have an adverse impact on the safety, important-to-safety, security, or emergency preparedness functions.

threat Natural or human-made occurrences, individuals, entities, or actions that have or indicate the potential to harm life, information, operations, the environment, 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 a safety, security, or emergency preparedness function susceptible to adverse impact.

Pre-Decisional

ACRONYMS AND ABBREVIATIONS

ADAMS	Agencywide Documents Access and Management System
BOP	balance of plant
CDA	critical digital asset
CERT	Community Emergency Response Team
CFR	*Code of Federal Regulations*
COL	combined operating license
CS	critical system
CSIRT	cyber security incident response team
CSP	cyber security plan
CST	cyber security team
DBT	design-basis threat
DG	draft regulatory guide
DHS	U.S. Department of Homeland Security
FERC	Federal Energy Regulatory Commission
HIDS	host-based intrusion-detection system
ICS	industrial control system
NIDS	network intrusion detection system
NEI	Nuclear Energy Institute
NIST SP	National Institute of Standards and Technology Special Publication
NPP	nuclear power plant
NRC	U. S. Nuclear Regulatory Commission
OMB	Office of Management and Budget
PMMD	portable media and mobile devices
RG	regulatory guide
SSEP	safety, security, and emergency preparedness
SRM	staff requirements memorandum
SSC	structure, system, and component

Pre-Decisional

REFERENCES[2]

1. U.S. *Code of Federal Regulations* (CFR), "Physical Protection of Plants and Materials," Part 73, Chapter 1, Title 10, "Energy."

2. CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."

3. CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

4. NRC Staff Requirements Memorandum (SRM) SECY, "Options and Recommendations for the Force-On-Force Inspection Program in Response to SRM-SECY-14-0088," Washington, DC, October 5, 2016. (ADAMS Accession No. ML16279A345)

5. U.S. Nuclear Regulatory Commission (NRC), Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," Washington, DC, February 2002. (ADAMS Accession No. ML020510635)

6. NRC, Order EA-03-086, "Design Basis Threat for Radiological Sabotage," Washington, DC, April 2003. (Safeguards information)

7. NRC, Regulatory Guide (RG) 5.83, "Cyber Security Event Notifications," Washington, DC, July 2015. (ADAMS Accession No. ML14269A388)

8. NRC, RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3, Washington, DC, July 2011. (ADAMS Accession No. ML102870022)

9. National Institute of Standards and Technology (NIST), NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, Gaithersburg, MD, September 2020.[3]

10. NRC, RG 5.71, "Cyber Security Programs for Nuclear Facilities," Revision 0, Washington, DC, January 2010. (ADAMS Accession No. ML090340159)

11. NRC Staff Requirements Memorandum (SRM)-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," Washington, DC, October 21, 2010. (ADAMS Accession

2 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site 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 The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov Documents that are withheld from the public can be requested by those individuals who have established a "need-to-know" and possess access permission to Official Use Only-Security-Related Information (OUO-SRI) or safeguards information (SGI) (or security clearance for classified documents).

3 Copies of National Institute of Standards and Technology documents may be obtained from the NIST Headquarters, 100 Bureau Drive, Gaithersburg, MD 20899, 301-975-2000, or electronically from its Web site: https://www.nist.gov/cyberframework.

Pre-Decisional

No. ML102940009)

12. NRC, NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," October 2004. (ADAMS Accession No. ML15111A054)

13. Nuclear Energy Institute (NEI), NEI 04-04, "Cyber Security Program for Power Reactors," Revision 1, Washington, DC, November 18, 2005.[4]

14. Zimmerman, R.P., NRC, Letter to Coyle, M.T., NEI, Subject: "NRC Acceptance of NEI 04-04, 'Cyber Security Program for Power Reactors,' Revision 1," December 23, 2005. (ADAMS Accession No. ML053320256)

15. NRC, NUREG/CR-7141, "The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors," Washington, DC, November 2014. (ADAMS Accession No. ML14323A203)

16. Institute of Electrical and Electronics Engineers (IEEE), IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Washington, DC, September 11, 2003.[5]

17. NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, Washington, DC, April 2010. (ADAMS Accession No. ML101180437)

18. NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, Washington, DC, July 2012. (ADAMS Accession No. ML12180A081)

19. Lui, C.H., NRC, Letter to Kline, D., NEI, Subject: "Nuclear Energy Institute 10-04, 'Identifying Systems and Assets Subject to the Cyber Security Rule,'" July 27, 2012. (ADAMS Accession No. ML12194A532)

20. NEI 13-10, Revision 6, "Cyber Security Control Assessments," August 2017. (ADAMS Accession No. ML17234A615).

21. NIST SP 800-82, "Guide to Industrial Control Systems Security," Gaithersburg, MD, September 29, 2008.

22. NIST SP 800-30, "Risk Management Guide for Information Technology Systems," Gaithersburg, MD, July 2002.

23. NIST SP 800-37, "Guide to Certification and Accreditation of Federal Information Systems," Gaithersburg, MD, May 2004.

---

4 Publications from the Nuclear Energy Institute (NEI) are available at its Web site: http://www.nei.org/ or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street, NW, Washington, DC 20006-3708, at (202) 739-800, or fax (202) 785-4019.

5 Copies of Institute of Electrical and Electronics Engineers (IEEE) documents may be purchased from the Institute of Electrical and Electronics Engineers Service Center, 445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855 or through the IEEE's public Web site at http://www.ieee.org/publications_standards/index.html.

Pre-Decisional

24. NRC, "Nuclear Regulatory Commission International Policy Statement," Federal Register, Vol. 79, No. 132, July 10, 2014, pp. 39415-39418.

25. NRC, Management Directive (MD) 6.6, "Regulatory Guides," Washington, DC, May 2, 2016 (ADAMS Accession No. ML18073A170).

26. International Atomic Energy Agency (IAEA) Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," Vienna, Austria, December 2011.[6]

27. IAEA Nuclear Energy Series NR-T-3.30, "Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants," Vienna, Austria, December 2020.

28. North American Electric Reliability Corporation, "Nuclear Power Plant 'Bright-Line' Survey," June 14, 2010.[7]

29. Federal Energy Regulatory Commission, Order 761, "Version 4 Critical Infrastructure Protection Reliability Standards", April 19, 2012.

30. NIST SP 800-61, "Computer Security Incident Handling Guide," Revision 2, Gaithersburg, MD, August 2012.

31. NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," Gaithersburg, MD, August 2006.

32. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Cyber Resiliency Review Implementation Guide," Volume 5, "Incident Management," 2016.

33. NRC, Management Directive (MD) 8.4, "Management of Facility-Specific Backfitting and Information Collection," Washington, DC, September 20, 2019. (ADAMS Accession No. ML18093B087)

34. NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems," Revision 1, Gaithersburg, MD, May 2010.

35. NIST SP 800-88, "Guidelines for Media Sanitization," Revision 1, Gaithersburg, MD, December 2014.

---

6 Copies of International Atomic Energy Agency (IAEA) documents may be obtained through its Web site: www.IAEA.Org/ or by writing the International Atomic Energy Agency, P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria. Telephone (+431) 2600-0, Fax (+431) 2600-7, or e-mail at Official.Mail@IAEA.Org.

7 Copies of NERC documents may be obtained by visiting the agency's Web site https://www.nerc.com; by writing to 1325 G Street, NW, Suite 600, Washington, DC 20005; or by calling (202) 400-3000.

Pre-Decisional

APPENDIX A

GENERIC CYBER SECURITY PLAN TEMPLATE

Note: In this appendix, any text shown in brackets is generic example text. The licensee or applicant should replace the example text with appropriate and applicable site-specific text. This cyber security plan (CSP) template uses Regulatory Guide (RG) 5.71 to show one acceptable means of meeting regulatory requirements. If the licensee selects other guidance for the basis of its CSP, it should modify references to RG 5.71 in Appendices A, B, and C to refer to the licensee-selected guidance.

[SITE] CYBER SECURITY PLAN

A.1 INTRODUCTION

The purpose of this [Licensee/Applicant] Cyber Security Plan (CSP, 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 that, if compromised, would adversely impact safety, security, or emergency preparedness (SSEP) 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 CSP. 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. The [Licensee/Applicant] acknowledges that the implementation of this plan does not alleviate [Licensee/Applicant]'s responsibility to comply with other regulations of the U.S. Nuclear Regulatory Commission (NRC).

The [Licensee/Applicant] complies with the requirements of 10 CFR 73.54 by implementing Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Power Reactors." RG 5.71 provides a method that the NRC staff considers acceptable for complying with the regulatory requirements in 10 CFR 73.54. 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 the [Licensee/Applicant] establishes/established a cyber security program to achieve high assurance that site digital assets or computer and communication systems and networks associated with 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 from cyber attacks of systems associated with the above functions:

Pre-Decisional

- 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 CSP, 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 defense-in-depth defensive strategies described in Section 3.1.5 of this plan, including the security controls described in Section 3.3 of RG 5.71, and (2) maintaining the program, as described in Section 4 of RG 5.71.

Documentation of the security controls in place for each CDA is available for inspection. Modifications to the CSP are conducted in accordance with 10 CFR 50.54(p). To comply with 10 CFR 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit," the [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 and 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.

Pre-Decisional

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 of CDAs. The networking arena includes knowledge of both sitewide and corporatewide 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:

- 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, 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

Pre-Decisional

- 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 CDAs

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 that, 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] conducted a dependency and pathway analysis to determine whether those systems or equipment are CSs; and

- [Licensee/Applicant]'s CST 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 in a CS or CDA security assessment:

- 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 and functions

Pre-Decisional

- known vulnerabilities about configuration and use of administrative (i.e., privileged) functions
- user-accessible security features or functions and how to effectively use those security features and 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, reviewed the following:

- direct and indirect connectivity pathways;
- infrastructure interdependencies; and
- the application of defense-in-depth defensive strategies, including security controls and other defensive measures;

The CST validated the above activities through comprehensive walkdowns that included the following:

- 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 the interdependencies of each CS and CDA with other CSs and CDAs and trust relationships between the CSs and 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 CS and CDA 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

Pre-Decisional

that provide connection validation equivalent to, or better than, physical walkdowns (e.g., use of a digital voltage meter, physical continuity validation). The validation activities should be linked to or documented in CS or CDA security assessments.

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, prevent, respond to, and recover from cyber attacks on CDAs. The defense-in-depth protective strategy consists of implementing the following:

- the defensive strategy described in Section C.6 of Appendix C to RG 5.71;
- the defensive architecture described in Section C.7 of Appendix C to RG 5.71; and
- the security controls implemented in accordance with Section 3.1.6 of this plan.

A.3.1.6 Application of Security Controls

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

- the defense-in-depth protective strategy described in Section 3.2 of RG 5.71;

  the physical and administrative security controls established by the [Site] physical security program. Physical barriers, such as locked doors, locked cabinets, and locating CDAs in the [Site] protected area or vital area;

- 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 accomplish one or more of the following for each CDA:

- implementing all of the security controls specified in Appendix B to RG 5.71

- for a security control that could not be applied, implementing alternative controls that mitigate the consequences associated with the threat or attack vectors associated with one or more of the security controls enumerated in Appendix B to RG 5.71 by accomplishing the following:

  - documenting the basis for employing alternative countermeasures

  - conducting and documenting an attack vector and attack tree analysis of the CDA and alternative controls to confirm that the countermeasures mitigate the same threat or attack vector 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

Pre-Decisional

- not implementing one or more of the security controls enumerated in Appendix B to RG 5.71 by accomplishing the following:
    - conducting attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented and
    - 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] conducted an effectiveness analysis, as described in Section 4.1.2, and vulnerability assessments or scans, as described in Section 4.1.3, of the CDAs to verify that the security program provides high assurance that CDAs are adequately protected from cyber attack, up to and including the DBT, and has closed any identified gaps. The outcomes of effectiveness analysis and vulnerability assessments or scans for a CDA should be associated with the documented CDA security assessment to provide an up-to-date view of the security posture of a CDA.

A.3.2 Incorporating the Cyber Security Program into the Physical Security 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 that 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 and 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 on the needs of both disciplines; and

Pre-Decisional

- periodically exercised 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 documented policies and implementing procedures to meet the security control objectives 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 the operation of one or more nuclear plants.

[Licensee/Applicant]'s procedures establish the specific responsibilities of the positions described in Section C.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;
- ongoing verification using established baseline configurations that CDAs are being protected commensurate with their safety and security significance;
- 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.

Pre-Decisional

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 CSP.

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 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 include, but are not limited to, periodic testing of the security controls; reevaluation of the capabilities of the adversaries consistent with the DBT; audits of the physical and cyber security programs and implementing procedures; safety and 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 do the following:

- 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;
- verify that existing security controls are functioning properly and are effective at protecting CDAs from cyber attack; and
- 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 that perform security functions are maintained according to the manufacturer's recommendations.

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 all CDAs to identify security deficiencies. The CST conducts assessments of security controls or 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 are identified that could potentially affect the

Pre-Decisional

effectiveness of the security program and security of the CDAs. 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 the vulnerabilities that could be exploited to compromise CDAs and 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 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.

[Licensee/Applicant] ensures that vulnerability assessments and scan reports and resulting mitigation actions are documented in or associated with the CDA's security assessment.

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 that incorporate cyber security requirements] 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 Section C.11 of Appendix C to RG 5.71. [Licensee/Applicant] implements a configuration and change management process, as described in Section 4.2 of this plan and Section C.11 of Appendix C to 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 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 in making changes, it used these configuration management procedures to avoid the introduction of additional vulnerabilities, weaknesses, or risks into the system. This process also ensures prompt 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

Pre-Decisional

[Licensee/Applicant]'s CST conducts a security impact analysis in accordance with Section 4.1.2 of this plan 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 defense-in-depth protective strategies, including 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] conducts 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 of this plan.

[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 before implementation, using a proven and accepted method, 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 that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among [Licensee/Applicant] entities, and compliance to reflect all modifications or additions; and

Pre-Decisional

- 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:

- plantwide and corporatewide 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 plantwide or corporatewide 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;
- identified potential pathways for attacks;
- recent cyber security studies or audits (to gain insight into areas of potential vulnerabilities); and
- identified infrastructure support (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] accomplishes the following:

- deploys the CDA into the appropriate level of the defense-in-depth protective strategy 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

Pre-Decisional

- 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] accomplishes the following:

- verifies that the CDA is deployed into the proper level of the defense-in-depth defensive security architecture described in Section 3.2.1 of RG 5.71;
- conducts 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

The [Licensee/Applicant]'s 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 safety or 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 on program effectiveness, and any actions taken as a result of recommendations from prior program reviews 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 operations. [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

Pre-Decisional

supporting technical documentation required to satisfy the regulations in 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.

Pre-Decisional

APPENDIX B

TECHNICAL SECURITY CONTROLS

Note: In this appendix, any text shown in brackets is generic example text. The licensee or applicant should replace the example text with appropriate and applicable site-specific text. Also, to maintain stability in security plans and automated tools supporting the implementation of Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Power Reactors," security controls will not be renumbered if a control is deleted. Rather, notations of security controls that have been deleted are maintained in the RG for historical purposes.

B.1 Access Controls

B.1.1 Access Control Policy and Procedures

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and implementing procedures offering administration, oversight, and management of the processes used for determining which entities require access rights to critical digital assets (CDAs).

Licensee/Applicant Activities

[Licensee/Applicant] develops, disseminates, and [annually] reviews and updates a formal, documented, CDA access control policy that 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 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, 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 media and mobile devices (PMMD), and use of external CDAs proprietary protocol visibility, third-party products and controls, and 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 passwords and key databases to prevent unauthorized access to master user and password lists;

Pre-Decisional

- 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

Control Intent

The intent of this control is to ensure the management and documentation of CDA accounts, including authorization, establishment, activation, modification, review, disablement, and removal of accounts.

Licensee/Applicant Activities

[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 an individual's job function changes to ensure that rights remain limited to the individuals job function;

- monitoring CDA accounts for atypical usage and reporting of such usage to designated [Licensee/Applicant] personnel;

- reviewing and documenting CDA accounts at a maximum interval consistent with the most recent version of Nuclear Energy Institute 03-12, "Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan," endorsed by the U.S. Nuclear Regulatory Commission (NRC);

- establishing processes for reissuing shared or group account credentials (if deployed) when individuals are removed from the group; and

- employing automated mechanisms that support CDA account management functions and enable CDA to automatically accomplish the following:

    - 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; and

Pre-Decisional

- 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 promptly investigate potential cyber attacks.

B.1.3 Access Enforcement

Control Intent

The intent of this control is to ensure enforcement of approved authorizations for logical and physical access to critical system (CS) and CDA resources in accordance with applicable access control policies. Approved authorizations will include access by direct or indirect means, regardless of physical proximity.

Licensee/Applicant Activities

[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 for 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

Control Intent

The intent of this control is to ensure enforcement of approved authorizations for controlling the flow of information within CSs, within CDAs, and between interconnected CSs and CDAs.

Pre-Decisional

Licensee/Applicant Activities

[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 the 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 a policy that allows or disallows information flows because of changing conditions or operational considerations;

- implementing mechanisms to prevent unauthorized data exfiltration; 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

Control Intent

The intent of this control is to ensure that one individual does not have functional control over, or responsibility for, all of the factors needed to perform an unauthorized, undesirable, or malicious activity.

Licensee/Applicant Activities

[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;

Pre-Decisional

- 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

- restricting security functions to the fewest number of users necessary to ensure the security of CDAs.

B.1.6 Least Privilege

Control Intent

The intent of this control is to ensure access rights are limited to the minimal functions required to perform the authorized activity.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- assigning the most restrictive set of rights and privileges or access needed by users, services, or automated processes for the performance of specified tasks;

- configuring CDAs to enforce the most restrictive set of rights and privileges or access needed by users, services, or automated processes; and

- implementing alternative controls and documenting the justification for alternative controls and countermeasures for increased auditing when 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

Control Intent

The intent of this control is to ensure implementation of measures to detect and respond to invalid user access attempts.

Licensee/Applicant Activities

[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 lockout 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. Alternately, other verification techniques or mechanisms that incorporate identity challenges are used; and

Pre-Decisional

- the access control policy documents the justification and details for alternative controls or countermeasures for those instances in which a CDA cannot support account or node locking or delayed login attempts. If a CDA cannot perform account or 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

Control Intent

The intent of this control is to ensure implementation of system use notifications to act as a deterrent for invalid or unauthorized use of a CDA.

Licensee/Applicant Activities

[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; and
    - unauthorized use of CDAs 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; and
- physical notices are installed in those instances in which a CDA cannot support system use notifications.

B.1.9 [DELETED]

Pre-Decisional

B.1.10 Session Lock

Control Intent

The intent of this control is to ensure enabling session lock functionality on a CDA or alternate measures that provide equivalent cyber security.

Licensee/Applicant Activities

[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; and
- maintain the session lock on a CDA until the user reestablishes access using identification and authentication procedures; or
- implement alternative controls and document the justification for alternative controls or countermeasures for those instances in which a CDA cannot support session locks or the following:
    - physically restrict access to the CDA
    - promptly monitor and record physical access to the CDA to detect and respond to intrusions,
    - 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
    - ensure that those individuals are trustworthy and reliable, in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants."

B.1.11 [DELETED]

B.1.12 Permitted Actions without Identification or Authentication

Control Intent

The intent of this control is to ensure the limitation and specific identification of all actions that can be performed on CDAs by unauthenticated or unidentified users during both normal and emergency conditions.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

Pre-Decisional

- 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

Control Intent

The intent of this control is to ensure the implementation of human-discernible, visible indications of the classification and sensitivity of CDA output that contains safeguards information, classified information, or sensitive information so that such output is appropriately handled.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- identifying and implementing standard naming conventions to identify 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 with 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 [DELETED]

B.1.15 Network Access Control

Control Intent

The intent of this control is to ensure network communication access and message traffic are approved and authorized or otherwise restricted.

Licensee/Applicant Activities

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

B.1.16 Open or Insecure Protocol Restrictions

Control Intent

The intent of this control is to ensure the elimination of vulnerabilities or mitigation of threat vectors associated with open or insecure protocols that can be exploited during a cyber attack.

Pre-Decisional

Licensee/Applicant Activities

[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 to a less secured posture.

B.1.17 Wireless Access Restrictions

Control Intent

The intent of this control is to ensure the implementation of adequate protections and procedures to minimize the cyber risk associated with the use of wireless technologies.

Licensee/Applicant Activities

[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 used;
- establishing usage restrictions, configuration and connection requirements, 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 defense-in-depth protective strategies, as articulated in RG 5.71; and
- conducting scans [no less frequently than once every week] or employing a wireless intrusion detection system 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

Control Intent

This control is intended to ensure that procedures are in place to promptly identify and remove or disable any unauthorized physical connections or interfaces.

Pre-Decisional

Licensee/Applicant Activities

[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 Media and Mobile Devices

Control Intent

The intent of this control is to ensure the establishment of usage restrictions, configuration requirements, connection requirements, and implementation procedures for PMMD. This control is also intended to ensure restricted usage of PMMD that could invalidate protections afforded by a security defensive architecture.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

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

B.1.20 Proprietary Protocol Visibility

Control Intent

The intent of this control is to ensure the implementation of countermeasures to protect a CDA from cyber attack because of the use of closed, unpublished, or vendor-proprietary protocols.

Licensee/Applicant Activities

[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), alternate 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

Control Intent

The intent of this control is to ensure the provision of other measures to address security vulnerabilities when third-party security solutions are not allowed because of vendor license and service agreements, and

Pre-Decisional

when loss of service support would occur if third-party applications are installed without vendor acknowledgment or approval.

Licensee/Applicant Activities

[Licensee/Applicant] ensures that, when third-party security solutions are not allowed because of vendor license and service agreements, and the loss of service support would occur if third-party applications were installed without vendor acknowledgement or approval, it implements alternative controls or countermeasures to mitigate vulnerabilities created by the lack of security functions provided by third-party products.

B.1.22 Use of External Systems

Control Intent

The intent of this control is to ensure CDAs are prohibited from access by, or communication with, external systems that are not within the same security level.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- ensuring that external systems cannot be accessed from safety, security, and important-to-safety CDAs or CSs;
- prohibiting external systems from accessing safety, security, and important-to-safety CDAs or CSs;
- ensuring that external systems cannot be accessed from CDAs located behind a one-way deterministic device in a manner that would result in a bypass that enables communications from lower levels to higher levels;
- prohibiting external systems from accessing CDAs located behind a one-way deterministic device; and
- prohibiting the use of an external system to access CDAs or to process, store, or transmit organization-controlled information except when [Licensee/Applicant] verifies the implementation of equivalent security measures on the external system.

B.1.23 Publicly Accessible Content

Control Intent

The intent of this control is to ensure public release of information is reviewed in advance to verify that it does not contain information that would aid an adversary in staging a cyber or physical attack on CDAs.

Pre-Decisional

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- designating individuals authorized to post information onto a [Licensee/Applicant] system that is publicly accessible;

- training 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; and

- 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

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementation procedures addressing requirements of cyber security auditing controls.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure the identification and enablement of appropriate auditing levels to support security incident and event analysis.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- determining and documenting the SSEP functions associated with a CDA, as described in Section C.3.1.3, that require auditing;

- defining the list of auditable events and frequency of auditing for each identified SSEP function, at a minimum auditing all CDA connections, user login/logouts, configuration/software/firmware

Pre-Decisional

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 when 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 [this Plan (Appendix A)].

B.2.3 Content of Audit Records

Control Intent

The intent of this control is to ensure that CDA event and activity logging is performed in a manner that provides the level of information necessary to support an after-the-fact cyber analysis of events and that the associated information is secured from tampering or destruction.

Licensee/Applicant Activities

[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, the outcomes of the events, and the identity of any individuals or subjects associated with 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

Control Intent

The intent of this control is to ensure collected and recorded CDA event and activity information is not lost because of insufficient storage capacity.

Pre-Decisional

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure event and activity log information is not lost or altered because of a full or partial loss of logging capabilities.

Licensee/Applicant Activities

[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 is documented;
- justification and details for alternate compensating security controls are documented when 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;
- [Licensee/Applicant] takes actions to preserve the audit logs for record retention requirements and after-the-fact investigations; and
- 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 and
    - auditing failures are treated as a failure of the CDA or security boundary device, and [Licensee/Applicant] will take action in accordance with the site procedures.

B.2.6 Audit Review, Analysis, and Reporting

Control Intent

The intent of this control is to ensure detection of suspicious, unauthorized, or malicious activity and alerting of personnel so that appropriate action may be taken to end the activity and mitigate or recover from any effects.

Pre-Decisional

Licensee/Applicant Activities

[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 a 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] SSEP 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 of, and response to, suspicious activities

B.2.7 Audit Reduction and Report Generation

Control Intent

The intent of this control is to ensure audit records containing events of interest are identified, analyzed, and available to support after-the-fact investigations.

Licensee/Applicant Activities

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

- provide CDA audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements, as well as after-the-fact investigations of cyber incidents, and does not alter the original content or time ordering of audit records; 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 when a CDA cannot support auditing reduction and report generation by providing this capability through a separate system.

B.2.8 Time Stamps

Control Intent

The intent of the control is to ensure log and event data collected by the various CDAs, systems, and devices can be correlated accurately to show the actual time sequence of associated events.

Licensee/Applicant Activities

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

Pre-Decisional

[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 through a trusted key management process.

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

B.2.9 Protection of Audit Information

Control Intent

The intent of this control is to ensure that activity and event log records are accurate, available, and protected from unauthorized access.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure implementation of controls and measures to protect CS and CDA identification methods and audit records in a manner that allows auditors and investigators to refute conclusively false claims by individuals denying execution of activities or actions.

Licensee/Applicant Activities

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

B.2.11 Audit Record Retention

Control Intent

The intent of this control is to ensure activity and event log information is retained for a timeframe sufficient to ensure that it meets both regulatory and cyber security requirements.

Licensee/Applicant Activities

[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.

Pre-Decisional

B.2.12 Audit Generation

Control Intent

The intent of this control is to ensure implementation of the capability to generate time-correlated and consolidated CDA activity and event logs.

Licensee/Applicant Activities

[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 sitewide (logical or physical) audit trail that is time correlated to within the [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

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementing procedures to address requirements of CDAs and communication protection controls.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure isolation of CDA application and security functions to prevent the compromise of the security functions.

Pre-Decisional

Licensee/Applicant Activities

[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 prevent the presentation of management-related functionality at an interface for nonprivileged users;
- 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 when a CDA cannot support security function isolation and taking all of the following actions:
    - physically restrict access to the CDA,
    - promptly monitor and record physical access to the CDA to detect and respond to intrusions,
    - use auditing and 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 authorized access to the CDAs are qualified, and
    - ensure that those individuals are trustworthy and reliable in accordance with 10 CFR 73.56.

Pre-Decisional

B.3.3 Shared Resources

Control Intent

The intent of this control is to ensure prevention of unauthorized and unintended information transfer by using shared system resources through the creation and maintenance of logical separation of Levels 3 and 4 from all other levels.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- configuring CDAs to prevent unauthorized and unintended information transfer by using 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

Control Intent

The intent of this control is to ensure prevention, limitation, or mitigation of the effects of denial-of-service attacks.

Licensee/Applicant Activities

[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;
- configuring CDAs to manage excess capacity, bandwidth, or other redundancies to limit the effects of information-flooding and saturation types of denial-of-service attack; and
- employing monitoring tools to detect indicators of denial-of-service attacks against CDAs and monitor resources to determine whether sufficient resources exist to prevent effective denial-of-service attacks.

B.3.5 [DELETED]

B.3.6 Transmission Integrity

Control Intent

The intent of this control is to ensure that the integrity of data is maintained as the data is passed to or from CDAs.

Pre-Decisional

Licensee/Applicant Activities

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

- configure CDAs to protect the integrity of transmitted information;
- employ cryptographic mechanisms to recognize changes to information during transmission and upon receipt, unless otherwise protected by alternate physical measures;
- implement mechanisms to prevent man-in-the-middle (MITM) attacks using the following methods:
  - Media Access Control Address Locking—[Licensee/Applicant] locks devices and ports using 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;
- implement monitoring to detect MITM and address resolution protocol poisoning; and
- implement alternative controls and document the justification for alternative controls or countermeasures when a CDA cannot support transmission integrity and implement all of the following:
  - physically restrict access to the CDA,
  - monitor and record physical access to the CDA to promptly detect and respond to intrusions,
  - use auditing and 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 authorized 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

Control Intent

The intent of this control is to ensure that the confidentiality of data is maintained as the data is passed to or from CDAs.

Licensee/Applicant Activities

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

- configure the CDAs to protect the confidentiality of transmitted information, such as not transmitting user credentials in clear text;

Pre-Decisional

- employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission and receipt unless otherwise protected by alternative physical measures; and

- implement alternative controls and document the justification for alternative controls or countermeasures when a CDA cannot internally support transmission confidentiality capabilities, including virtual private networks, or implement all of the following:

    - physically restrict access to the CDA,

    - monitor and record physical access to the CDA to promptly detect and respond to intrusions,

    - use auditing and 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 authorized access to the CDA are qualified, and

    - ensure that those individuals are trustworthy and reliable, in accordance with 10 CFR 73.56.

B.3.8 Trusted Path

Control Intent

The intent of this control is to ensure prevention of user credential exposure during the authentication and user login process.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure cryptographic measures are employed to protect the confidentiality and integrity of data stored, transmitted, or received by CSs and CDAs and that the keys employed are effectively protected from discovery, decryption, or compromise.

Licensee/Applicant Activities

[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"].

Pre-Decisional

B.3.10 Use of Cryptography

Control Intent

The intent of this control is to ensure implementation of cryptographic measures that are robust, resilient, and highly resistant to cryptanalysis to protect the confidentiality and integrity of data stored, transmitted, or received by CSs and CDAs.

Licensee/Applicant Activities

[Licensee/Applicant] configures CDAs to implement cryptographic mechanisms that comply with [FIPS 140-2].

B.3.11 Unauthorized Remote Activation of Services

Control Intent

The intent of this control is to ensure prevention of unauthorized remote access to a CDA's information-sharing collaboration services and hardware resources.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure proper transmission to or from CDAs of information security markings, tags, or other identifiers.

Licensee/Applicant Activities

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

B.3.13 Public Key Infrastructure Certificates

Control Intent

The intent of this control is to ensure the establishment of policies and procedures on the appropriate use, generation, acceptance, and verification of public key infrastructure (PKI) certificates.

Pre-Decisional

Licensee/Applicant Activities

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

B.3.14 Mobile Code

Control Intent

The intent of this control is to ensure control or prohibition of mobile code use on CDAs.

Licensee/Applicant Activities

[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)

Control Intent

The intent of this control is to ensure implementation and use of secure domain name service (DNS) services.

Licensee/Applicant Activities

[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, enable verification of a chain of trust among parent and child domains

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

Control Intent

The intent of this control is to ensure implementation and use of secure DNS services in licensee-operated DNS servers and in the CDAs that use those services.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

Pre-Decisional

- configuring the systems that provide 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

Control Intent

The intent of this control is to ensure the implementation and use of secure DNS services in licensee-operated servers and in the CDAs that use those services.

Licensee/Applicant Activities

[Licensee/Applicant] configures the systems that collectively provide name/address resolution services for a logical organization to be fault tolerant and segregate services (i.e., implement role separation).

B.3.18 Session Authenticity

Control Intent

The intent of this control is to ensure communications among CSs and CDAs, traversing an unsecure network, are established and maintained using applicable controls and measures to verify the authenticity of the session participants at session initiation and to provide security for the duration of the session.

Licensee/Applicant Activities

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

B.3.19 [DELETED]

B.3.20 Protection of Information at Rest

Control Intent

The intent of this control is to ensure information at rest is protected against unauthorized disclosure or modification.

Licensee/Applicant Activities

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

Pre-Decisional

B.3.21 Heterogeneity/Diversity

Control Intent

The intent of this control is to ensure avoidance of common exploitable vulnerabilities and flaws by introducing diversity in manufacturers and models.

Licensee/Applicant Activities

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

B.3.22 Fail in Known State

Control Intent

The intent of this control is to ensure the CDA will fail in a known state to protect the SSEP function.

Licensee/Applicant Activities

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

- ensure that CDAs fail in a known state to prevent the CDA's failure from adversely impacting SSEP functions; and
- 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

Control Intent

The intent of this control is to ensure the development and dissemination of a formal, complete, coherent, and comprehensive identification and authentication policy with associated implementing procedures.

Licensee/Applicant Activities

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

- a formal, documented identification and authentication policy that 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:

Pre-Decisional

- uniquely identifying each user and process acting on behalf of a user;
- verifying the identity of each user and process 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 the user identifier after a maximum of [30 days] of inactivity;
- disabling the 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 or refreshing authenticators [annually].

B.4.2 User Identification and Authentication

Control Intent

The intent of this control is to ensure the establishment of strong authentication mechanisms and procedures to prevent unauthorized CDA access and usage. This control is also intended to ensure only legitimate, authorized personnel are allowed to gain user access to CDAs and only such access as their job functions require.

Licensee/Applicant Activities

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

- implement identification and authentication technology to uniquely identify and authenticate individuals and processes acting on behalf of users interacting with CDAs 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;
- ensure that the authentication technology employs strong multifactor authentication using protected processing levels;
- implement alternative controls and document the justification for alternative controls or countermeasures when a CDA cannot support user identification and authentication and implement all of the following:
    - physically restrict access to the CDA;

Pre-Decisional

- monitor and record physical access to the CDA to promptly detect and respond to intrusions;
- use auditing and 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;
- ensure that those individuals are trustworthy and reliable in accordance with 10 CFR 73.56.

- implement 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.
- 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

Control Intent

The intent of this control is to ensure password requirements provide protection against unauthorized access.

Licensee/Applicant Activities

[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;

Pre-Decisional

- 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];
- 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; and
- authority to change master passwords is limited to authorized personnel.

B.4.4 Nonauthenticated Human-Machine Interaction Security

Control Intent

The intent of this control is to ensure implementation of physical security measures to ensure that access to, and the use of, CSs and CDAs is limited to authorized personnel and that actions performed on the CS and CDA can be tracked and attributed to the specific individuals.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- ensuring that, when a human-machine interaction (HMI) for a CDA cannot support authentication because of operational requirements, adequate physical security controls exist that require that operators be both authorized and properly identified and be monitored so that operator actions are audited and recorded;
- controlling access to nonauthenticated human machine interactions (NHMIs) to avoid hampering HMIs while maintaining security of the NHMI and ensuring that access to the NHMI is limited to only authorized personnel;
- verifying that authentication, session lock, or session termination controls do not adversely affect SSEP functions; 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 meet auditing requirements.

B.4.5 Device Identification and Authentication

Control Intent

The intent of this control is to ensure secure management of unique identifiers.

Licensee/Applicant Activities

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

Pre-Decisional

- implement and document technology that identifies and authenticates devices (i.e., tester) before those devices establish connections to CDAs; and

- implement alternative controls and document the justification for alternative controls or countermeasures when a CDA cannot support device identification and authentication (e.g., serial devices), and implement all of the following:

    - physically restrict access to the CDA;

    - monitor and record physical access to the CDA to promptly detect and respond to intrusions;

    - use auditing and validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDA;

    - ensure that authorized 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.4.6 Identifier Management

Control Intent

The intent of this control is to ensure secure management of unique identifiers.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure secure management of unique authenticators.

Licensee/Applicant Activities

[Licensee/Applicant] manages CDA authenticators by performing all of the following:

- defining initial authenticator content, such as 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;

Pre-Decisional

- changing default authenticators upon CDA installation; and
- changing or refreshing authenticators [annually].

B.4.8 Authenticator Feedback

Control Intent

The intent of this control is to ensure mechanisms are in place to prevent accidental or unintentional disclosure of authenticator or authentication mechanism information.

Licensee/Applicant Activities

[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 CDAs do not provide information that would allow an unauthorized user to compromise the authentication mechanism.

B.4.9 Cryptographic Module Authentication

Control Intent

The intent of this control is to ensure the use of well-tested, effective, and proven cryptographic technology where cryptographic functionality is required.

Licensee/Applicant Activities

[Licensee/Applicant] ensures that CDAs authenticate cryptographic modules in accordance with [FIPS 140-2].

B.5 System Hardening

B.5.1 Removal of Unnecessary Services and Programs

The intent of this control is to ensure the CDA is hardened and reduces the available attack surface through the elimination of potentially vulnerable and exploitable software, hardware, and network elements.

Licensee/Applicant Activities

[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. The documentation can be used as the baseline configuration of the CDA in accordance with the baseline configuration security control in Section C.11.3 of Appendix C to RG 5.71 and should be reflected in the CDA security assessment.

Pre-Decisional

[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 Section C.3.2 of Appendix C to RG 5.71.

[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);
- 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

Pre-Decisional

- games.

B.5.2 Host Intrusion Detection System

Control Intent

The intent of this control is to ensure automated mechanisms are provided to detect the unauthorized modification of a system's software, data, or configuration settings and unauthorized or abnormal activities.

Licensee/Applicant Activities

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

- configure the host-based 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 usage, and process permissions, to enable the system to detect cyber attacks up to and including the DBT;

- configure the 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 CDA safety, security, and emergency preparedness functions;

- configure security logging storage devices as "append only" to prevent alteration of records on those storage devices; and

- 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

Control Intent

The intent of this control is to ensure maintenance of a CDA's file system and executable processes at the lowest level for the CDA to perform its intended function and to protect against unauthorized modification.

Licensee/Applicant Activities

[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;

Pre-Decisional

- document the changing or disabling of access to files and functions; and

- validate that baseline permission and security settings are not altered after modifications or upgrades.

B.5.4 Hardware Configuration

Control Intent

The intent of this control is to ensure the elimination or reduction of available vulnerabilities and communication attack vectors that an attacker could exploit through a CDA's hardware component.

Licensee/Applicant Activities

[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 provide engineered barriers. If both methods physically and through software are available to disable unneeded capabilities, then physically disabling the capability should be the preferred method unless it would cause improper operation of the CDA; and

- password protect the basic input-output system from unauthorized changes;

- document mitigation measures when password protection of the basic input-output system is not technically feasible;

- document the hardware configuration (e.g., switch settings, bus cards, software and firmware versions; remove or disable unneeded hardware and input/output ports);
.
- 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; and

- 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

Control Intent

The intent of this control is to ensure the application of security-related patches and software updates to CDAs to eliminate or mitigate identified security vulnerabilities.

Licensee/Applicant Activities

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

- the patch management program, update process, and individuals responsible for installation;

Pre-Decisional

- 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;

- 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 when 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 or device for testing and validation before installing on production systems; and

- all updates for security impact.

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

Pre-Decisional

APPENDIX C

OPERATIONAL AND MANAGEMENT SECURITY CONTROLS

Note: In this appendix, any text shown in brackets is generic example text. The licensee or applicant should replace the example text with appropriate, applicable, site-specific text. Also, to maintain stability in security plans and automated tools supporting the implementation of Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Power Reactors," security controls will not be renumbered if a control is deleted. Rather, notations of security controls that have been deleted are maintained in the RG for historical purposes.

OPERATIONAL CONTROLS

C.1 Media Protection

C.1.1 Media Protection Policy and Procedures

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated procedures to address requirements of media protection controls.

Licensee/Applicant Activities

[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 [Licensee/Applicant] entities, and compliance for each information category, as defined by the site policies, and ensures that any media that 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

Control Intent

The intent of this control is to ensure access to portable media and mobile devices containing sensitive critical digital asset (CDA) data or security information is controlled, monitored, and audited.

Pre-Decisional

Licensee/Applicant Activities

[Licensee/Applicant] documents and restricts access to CDA media to authorized individuals only. CDA media include both digital media (e.g., diskettes, magnetic tapes, external or removable hard drives, flash or 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 and Marking

Control Intent

The intent of this control is to ensure the establishment of mechanisms and procedures to enable personnel to determine the sensitivity and classification of information on removable media and in CDA output.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure media containing sensitive information are physically protected and stored in accordance with their sensitivity levels and that access to such media is restricted to authorized parties.

Licensee/Applicant Activities

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

C.1.5 Media Transport

Control Intent

The intent of this control is to ensure that data related to critical systems (CSs) or CDAs are adequately protected when in transport.

Pre-Decisional

Licensee/Applicant Activities

[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 individuals 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 the [Licensee/Applicant]-defined system of records.

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

C.1.6 Media Sanitization and Disposal

Control Intent

The intent of this control is to ensure the appropriate destruction or disposal of media and verify media sanitization.

Licensee/Applicant Activities

[Licensee/Applicant] sanitizes CDA media, both digital and nondigital, before disposal or release for reuse. [Licensee/Applicant] [follows the guidance in National Institute of Standards and Technology (NIST) SP 800-88 (Ref. 35)] to sanitize CDA media. The information is destroyed by a method that precludes reconstruction by means available to the design-basis threat (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

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and implementation of associated procedures to address requirements of personnel security.

Pre-Decisional

Licensee/Applicant Activities

[Licensee/Applicant]'s reviewing official grants unescorted access authorization to those individuals who have access to, extensive knowledge of, or administrative control of CDAs or communication systems that can adversely impact CDAs or SSEP 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

Control Intent

The intent of this control is to ensure the implementation of procedures providing prompt retrieval of credentials and authenticators and termination of all accounts and access rights when personnel are terminated or transferred.

Licensee/Applicant Activities

[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:

- disables all CDA and system access and terminates or revokes any authenticators or credentials associated with the individual;
- 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 the terminated individual.

C.3 System and Information Integrity

C.3.1 System and Information Integrity Policy and Procedures

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementing procedures to address requirements of system and information integrity controls.

Pre-Decisional

Licensee/Applicant Activities

[Licensee/Applicant] develops, disseminates, 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 accomplish the following:

- detect malicious or suspicious access control or networking anomalies occurring at established defensive-level boundaries and within security levels;

- alert appropriate staff to the detected malicious or suspicious activity using a secure communications mechanism that is protected from the network being monitored;

- isolate and contain malicious activity;

- neutralize malicious activity;

- centralize logging of cyber security events to support correlations;

- provide secure monitoring and management of security mechanisms;

- provide time synchronization for all security-related devices; and

- provide high assurance that the physical and logical security of the monitoring network (or systems and CDAs) matches or exceeds, and differs from, the systems and CDAs or networks being monitored.

C.3.2 Flaw Remediation

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of procedures for monitoring security alerts and implementing security updates in a manner that guarantees both effective remediation and proper SSEP functionality.

Licensee/Applicant Activities

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

- identifying the security alerts and vulnerability assessment process;

- communicating vulnerability information;

Pre-Decisional

- correcting the flaw expeditiously using the configuration management process;

- correcting security flaws in CDAs; and

- performing vulnerability scans and assessments of the CDA to verify that the flaw has been eliminated before the CDA is implemented.

Before implementing corrections, [Licensee/Applicant] documents and tests software and firmware updates related to flaw remediation to determine the effectiveness and potential side effects on CDAs. [Licensee/Applicant] captures flaw remediation information in its corrective action program.

C.3.3 Malicious Code Protection

Control Intent

The intent of this control is to ensure prevention, detection, and elimination of malware infection of security boundary devices, CSs and CDAs, workstations, servers, and portable media and mobile devices (PMMD), including along the attack pathways(s).

Licensee/Applicant Activities

[Licensee/Applicant] establishes, deploys, and documents real-time malicious code protection mechanisms at security boundary device entry and exit points (e.g., firewalls, digital media zones, data diodes, malware scanning stations, data transfer guards), CDAs (if applicable), workstations, servers, and mobile computing devices (e.g., calibrators and maintenance and test equipment laptops) on the network to detect and eradicate malicious code resulting from the following:

- data communication between systems, CDAs, removable media, portable storage devices, 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;

- real-time scans of files from external sources are performed and whitelisting is employed as the files are downloaded, opened, or executed; and

- 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

Pre-Decisional

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:

- CDAs prevent users from circumventing malicious code protection capabilities; and
- 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 to operate 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

Control Intent

The intent of this control is to ensure establishment and maintenance of an adequate plantwide cyber surveillance capability on networks, systems, and devices affecting CSs and CDAs.

Licensee/Applicant Activities

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

- monitor events on the CDAs;
- detect cyber attacks and indicators of potential cyber attacks on CDAs and along the attack pathways(s);
- detect and block unauthorized local, network, and remote connections;

  retain event logs in accordance with information retention requirements;
- identify unauthorized use of the CDAs;
- monitor devices that are deployed to provide visibility across CDAs for the following capabilities:
  - collect information to detect attacks, unauthorized behavior and access, and authorized access.
  - track specific types of transactions of interest to [Licensee/Applicant]; and

Pre-Decisional

- adjust monitoring tools and techniques as threat agents constantly change and adapt their tactics to circumvent defenses and countermeasures.

[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, "Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan," 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] analyzes and documents outbound communications traffic at the external boundary of CDAs (i.e., system perimeter) and at selected interior points within the CSs' infrastructure to detect covert exfiltration of information.

Pre-Decisional

[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

Control Intent

The intent of this control is to ensure the use of credible information sources to receive prompt information about security threats and vulnerabilities and the use of that information to take prompt and appropriate action to mitigate any potential security effects to CDAs.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- receives prompt 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 maintains a copy of these documents;

- independently evaluates and determines the need, severity, methods, and timeframes for implementing security directives consistent with the security controls for the CDA (Section 3.1 of [this Plan (Appendix A)]); and

- within established timeframes set by the licensee or as directed by the NRC, accomplishes the following:

    - 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

Control Intent

The intent of this control is to ensure CDAs' security functions are in place; are working as intended; and have not been modified, degraded, corrupted, or subverted.

Pre-Decisional

Licensee/Applicant Activities

[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 when 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;
- individuals determined to be trustworthy and reliable 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 prompt detection and response to intrusions); and
- auditing and validation measures (e.g., security officer rounds and periodic monitoring of tamper seals).

C.3.7 Software, Firmware, and Information Integrity

Control Intent

The intent of this control is to ensure CDA software, firmware, and data are protected from unauthorized changes.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- detecting and documenting unauthorized changes to software, firmware, and information;
- employing hardware access controls (e.g., hardwired switches), where technically feasible, to prevent unauthorized software and firmware changes;
- reassessing and documenting the integrity, operation, and functions of software, firmware, and information by performing regular integrity, operational, and functional

Pre-Decisional

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 notify 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;
- implementing cryptographic mechanisms (e.g., hash algorithm, digital signatures, or other equivalent methods) to detect unauthorized changes to software, firmware, and information;
- 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

Control Intent

The intent of this control is to ensure that CDA functionality is not compromised through the manual or automatic input of invalid or potentially malicious data.

Licensee/Applicant Activities

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

- the capability to input information to CDAs is restricted to only authorized sources and
- 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

Control Intent

The intent of this control is to ensure CDA error conditions and associated responses do not provide a means for unintended disclosure of sensitive information.

Pre-Decisional

Licensee/Applicant Activities

[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; and
- inclusion of sensitive information, such as passwords, user names, and personal identifiable information, in error logs or associated administrative messages is prohibited.

C.3.10 Information Output Handling and Retention

Control Intent

The intent of this control is to ensure CDA output handling or retention is not improper, leading to disclosure of sensitive information to unauthorized personnel.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure CDAs can be returned to intended functionality in the event of a failure or compromise.

Licensee/Applicant Activities

[Licensee/Applicant] protects the availability of CDAs through compliance with technical specifications, preventive maintenance programs, Maintenance Rule programs, security plans, emergency plans, or its 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;
- consideration of the mean time to failure for components in specific operational environments; and
- having adequate inventory of essential spare parts.

Pre-Decisional

C.4 Maintenance

C.4.1 System Maintenance Policy and Procedures

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated procedures to address the requirements of system maintenance.

Licensee/Applicant Activities

[Licensee/Applicant] developed, disseminated, and [annually] reviews and updates 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 that 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 public health and safety by exposure to radiation (vital areas may also contain equipment or systems that would be required to function to protect public health and safety following such failure, destruction, or release) (see 10 CFR 73.2, "Definitions"); and
    - public access area: locations outside the physical control of the plant.

C.4.2 Maintenance Tools

Control Intent

The intent of this control is to ensure that microprocessor-based tools, devices, and equipment or computer-readable media used for CDA maintenance and support activities are not maliciously or unintentionally used to transport malware or to launch a cyber attack.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

Pre-Decisional

- 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 or 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

Control Intent

The intent of this control is to ensure the documentation and monitoring of personnel given authorization to perform CDA maintenance activities, as well as the documentation and monitoring of escorted maintenance and service personnel activities to ensure that they take no inappropriate or malicious actions.

Licensee/Applicant 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 [an automated mechanism or a 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

Pre-Decisional

C.5 Physical Protection

C.5.1 Physical Protection Policies and Procedures

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and implementing procedures to address the physical protection of CDAs outside of the protected area.

Licensee/Applicant Activities

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

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

C.5.2 Third-Party/Escorted Access

Control Intent

The intent of this control is to ensure the strict monitoring, control, and restriction of CDA physical access to authorized third-party personnel who have been deemed trustworthy.

Licensee/Applicant Activities

[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.

Pre-Decisional

C.5.3 Physical Protection

Control Intent

The intent of this control is to ensure implemented CS and CDA protection strategies address physical threats to CDAs.

Licensee/Applicant Activities

[Licensee/Applicant] secures and documents physical access to CDAs. Physical security controls (e.g., physical, locked, drivers) are employed to limit access to CDAs.

C.5.4 Physical Access Authorizations

Control Intent

The intent of this control is to ensure maintenance of an access authorization program.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- developing and maintaining access lists 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 removing individuals from the access lists when access is no longer required; and

- designating officials within the organization to review and approve the above access lists and authorization credentials, consistent with the access authorization program in accordance with 10 CFR 73.56.

C.5.5 Physical Access Control

Control Intent

The intent of this control is to ensure an adversary is prevented from gaining unauthorized physical and logical access to CDAs.

Licensee/Applicant Activities

[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

Pre-Decisional

- 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

Control Intent

The intent of this control is to ensure the protection of physical access to communication infrastructure.

Licensee/Applicant Activities

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

C.5.7 Access Control for Display Medium

Control Intent

The intent of this control is to ensure the prevention of the unintended and unauthorized disclosure of sensitive information through its visual presentation on a CDA-driven display.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure detection of and response to all physical access to CDAs and security boundaries.

Licensee/Applicant Activities

[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;

Pre-Decisional

- monitoring real-time physical intrusion alarms and surveillance equipment;
- employing automated mechanisms to assess and recognize potential intrusions and initiate appropriate response actions; and
- providing adequate lighting for access monitoring devices (e.g., cameras).

C.5.9 Visitor Control Access Records

Control Intent

The intent of this control is to ensure identification, authorization, and monitoring of visitors.

Licensee/Applicant Activities

[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 before entry; and
- escorting visitors and monitoring visitor activity to prevent adverse impacts to SSEP functions.

C.6 Defense-in-Depth Defensive Strategy

Control Intent

The intent of this control is to ensure that the basis for the entire cyber security program is adequately met by the elements of a defense-in-depth protective strategy.

Licensee/Applicant Activities

[Licensee/Applicant] employs and documents its [Site] defensive security strategy, which includes the following elements:

- implement management, operational, and technical security controls in Appendices B and C to RG 5.71 to detect, delay, mitigate, and recover from a cyber attack;
- implement defense-in-depth security architecture as described in Section C.3.2.1 of this guide; and
- use multiple layers of defensive security controls placed throughout the protected network and systems with the intent of providing overlapping defenses if a control fails or a vulnerability is exploited. Therefore, each implemented security control can serve an additional purpose of contributing another defensive control to the defense-in-depth security architecture.

Pre-Decisional

C.7 Defense-in-Depth Defensive Security Architecture

Control Intent

The intent of this control is to ensure the implementation of a defense-in-depth protective strategy that includes defensive security architecture, establishing the core of the cyber security program.

Licensee/Applicant Activities

[Licensee/Applicant] implements and documents a defensive architecture that includes the following elements:

- identify the logical boundaries for data transfer and associated communication protocols. The architecture defines the level of connectivity permitted between levels and individual CDAs;
- allocate the highest degree of cyber security protection to CDAs that carry out safety and security functions and protect those CDAs from attacks emanating from lower defensive levels using a consequence-based graded approach;
- allocate CDAs that provide data acquisition functions to at least the second highest security level of protection;
- allow only one-way data flow from the highest security level to the next lower security level;
- identify the protective controls associated within each security level; this includes the secure management (confidentiality, integrity, and availability) of data within a security level;
- afford any non-safety system that has bidirectional communication with a safety system with the same level of protection as the safety system;
- prevent remote access to CDAs located at the highest security level;
- prevent spoofing of addresses from one security level to another;
- initiate communications from digital assets at lower security levels to CDAs at higher security levels on a "deny-all, permit-by-exception" basis, with the exceptions supported by a complete justification and security risk analysis; and
- move data, software, firmware, and devices from lower levels of security to higher levels of security using a documented validation process or procedure that 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:

Pre-Decisional

- physically and logically secure and harden devices to prevent unauthorized access or manipulation;

- ensure that access to such devices is controlled and monitored in accordance with [Licensee/Applicant] policies and procedures;

- configure devices to provide only essential capabilities necessary to perform their functions and specifically prohibit or restrict the use of any other available functions or features, including ports, protocols, and services;

- employ secure management communications and encryption in accordance with Appendix B to RG 5.71;

- provide logging and alert capabilities;

- monitor boundary control devices for anomalous activity and inappropriate use;

- ensure that personnel responsible for managing these devices subscribe to security advisories and other relevant sources that provide up-to-date information about boundary control device vulnerabilities, so relevant patches, updates, and protective actions can be taken;

- take measures to ensure that operational failures of boundary protection mechanisms would not compromise the [Licensee/Applicant] defensive strategy. These measures include, but are not limited to, implementing redundancy and failover strategies or backing up configuration settings for devices;

- review device configurations [quarterly];

- provide intrusion detection and prevention capabilities;

- detect and prevent malware from moving between boundaries;

- possess 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, contain a rule set that, at a minimum, accomplishes the following:

    - is configured to deny traffic, except that which is explicitly authorized;

    - provides protocol, source, and destination filtering such as Internet protocol (IP) addresses, MAC addresses, transmission control protocol (TCP) ports, and user datagram protocol ports (UDP);

    - 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;

Pre-Decisional

- 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;
- ensures that changes to configuration parameters, enabled services, and rule set are in accordance with the section for the configuration change control in this cyber security plan;
- receives time synchronization from a trusted and dedicated source existing on the security network, attached directly to the CDA or through a Simple Network Time Protocol 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 who are appropriately trained in such analysis to detect malicious and anomalous activity;
- is tuned to detect anomalous activity and communication;
- is updated [quarterly];

Pre-Decisional

- 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 higher security levels protected by a one-way deterministic device; and

- employs measures to prevent viruses or other malicious or unwanted programs from propagating information between security levels.

C.8 Incident Response

Control Intent

The intent of this control family is to ensure it enables the detection, deterrence, response to, and recovery from a cyber attack.

Licensee/Applicant Activities

[Licensee/Applicant] establishes, implements, and documents to ensure that 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 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's/applicant's corrective action program evaluates, tracks, manages, provides corrective action to, and documents cyber attacks.

[Licensee/Applicant] procedures that govern response to cyber events direct prompt 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 of 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;

- verify that surrounding or interconnected CDAs, networks, and support systems are not contaminated, degraded, or compromised; and

Pre-Decisional

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 10 CFR 73.77, "Cyber Security Event Notifications"; Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73, "Physical Protection of Plants and Materials"; and as further described in Section C.8.6.

C.8.1 Incident Response Policy and Procedures

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementing procedures to address requirements of incident response.

Licensee/Applicant Activities

[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 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;

    - if 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 that 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

Pre-Decisional

plans, business continuity or emergency plans] and that changes 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 (CST)
- operations
- engineering
- information technology
- human resources
- system support vendors
- management
- legal

C.8.2 Incident Response Training

Control Intent

The intent of this control is to ensure effective training for personnel who must respond to cyber incidents.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure verification of the effectiveness of the incident response capability through testing and drills.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- testing and conducting drills of the incident response capability for CDAs [at least annually];

Pre-Decisional

- 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 drill 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

Control Intent

The intent of this control is to ensure [Licensee/Applicant] establishes a cyber security incident response team (CSIRT) that is capable of addressing cyber incidents effectively.

Licensee/Applicant Activities

[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 the existing incident handling program];

- incorporating lessons learned from ongoing incident handling activities into incident response procedures, contingency planning, training, and testing or exercises, and implementing the resulting changes accordingly;

- forming an integrated CSIRT;

- 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 responses 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 and recovery process;

Pre-Decisional

- 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;

- description 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 plantwide and corporatewide networks.

- nuclear facility operations, engineering, and safety—This includes knowledge of overall facility operations and plant technical specifications. The 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 plant SSEP 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 areas. 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

Pre-Decisional

- corporate public relations
- corporate legal

Incident data collected include 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 affected
- brief description of incident
- impact on organization
- measures to prevent recurrence
- references

C.8.5. Incident Monitoring

Control Intent

The intent of this control is to ensure security incidents are documented and analyzed.

Licensee/Applicant Activities

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

C.8.6 Incident Reporting

Control Intent

The intent of this control is to ensure cyber events are reported in accordance with regulations.

Licensee/Applicant Activities

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 NRC.

[Licensee/Applicant] is required to comply with requirements of 10 CFR 73.77. RG 5.83, "Cyber Security Event Notifications," provides guidance on acceptable approaches and methodologies for categorizing certain cyber security events, as well as the process for conducting notifications and submitting written security follow-up reports to the NRC for cyber security event notifications.

Pre-Decisional

C.8.7 Incident Response Assistance

Control Intent

The intent of this control is to ensure resources for a 24/7 incident response capability are available.

Licensee/Applicant Activities

[Licensee/Applicant] provides competent and trained incident response support personnel who are available all year, 24 hours a day, to offer advice and assistance to users of CDAs in response to the 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

Control Intent

The intent of this control is to ensure management support for and adequate resources to implement an effective incident response capability.

Licensee/Applicant Activities

[Licensee/Applicant] developed, implemented and reviews [annually] an incident response plan that accomplishes the following:

- 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 Section C.8.6 of this Appendix;
- 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 to 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; communicates incident response plan changes to plant personnel, including incident response personnel; and protects the incident response plan from unauthorized disclosure and modification.

Pre-Decisional

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

C.9.1 Contingency Planning Policy and Procedures

Control Intent

The intent of this control is to ensure development, documentation, and deployment of policies and associated implementing procedures to address requirements of contingency planning.

Licensee/Applicant Activities

[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.

Pre-Decisional

C.9.2 Contingency Plan

Control Intent

The intent of this control is to ensure contingency planning supports the capability for responding to a contingency event and to maintain SSEP functions.

Licensee/Applicant Activities

[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 a compromise, disruption, or failure effects a CDAs and restoring those CDAs to normal operation;

- 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 needed 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 so that, in the event of a loss of processing within a CDA or a loss of communication with operational facilities, CDAs will execute predetermined actions (e.g., fail safe).

C.9.3 Contingency Plan Testing

Control Intent

The intent of this control is to ensure implementation testing and drills to verify the effectiveness of the contingency plan.

Licensee/Applicant Activities

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

- test, exercise, and document the contingency plan [at least annually] to verify its effectiveness and the organization's readiness to execute this plan;

- review the contingency plan test and exercise results and initiate appropriate corrective actions;

- coordinate contingency plan testing and exercises with [Licensee/Applicant] elements responsible for related plans;

Pre-Decisional

- test, exercise, and document the contingency plan at emergency and backup sites to familiarize contingency personnel with these facilities and their available resources and to evaluate the [Site's] capabilities to support contingency operations;

- employ automated mechanisms such as modeling and simulations to thoroughly and effectively test and exercise the contingency plan by providing a more complete coverage of contingency issues and selecting more realistic test and exercise scenarios and environments;

- include recovery and reconstitution of CDAs as part of contingency plan testing;

- establish and document 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

- use scheduled and unscheduled system maintenance activities, including responses to CDA component and system failures, as an opportunity to test or exercise the contingency plan.

C.9.4 Contingency Plan Training

Control Intent

The intent of this control is to ensure implementation of an effective training plan for all personnel with roles in the contingency plan.

Licensee/Applicant Activities

[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 such as modeling and simulations to thoroughly and effectively test and drill the contingency plan by providing more complete coverage of contingency issues; and

- selecting realistic test and drill scenarios and environments, effectively stressing the CDAs.

Pre-Decisional

C.9.5 Alternate Storage Site and Location for Backups

Control Intent

The intent of this control is to establish a secure alternate storage site and maintain the capability for CDA restoration.

Licensee/Applicant Activities

[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 taking the following actions:

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

C.9.6 CDA Backups

Control Intent

The intent of this control is to ensure procedures are established to verify the availability of all CDA backups.

Licensee/Applicant Activities

[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 [on a scheduled basis] 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;

Pre-Decisional

- 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

Control Intent

The intent of this control is to ensure that the capability to recover and restore CDAs to a known secure state is established.

Licensee/Applicant Activities

[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 CDAs are performing correctly.

C.10 Awareness and Training

C.10.1 Cyber Security Awareness and Training

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementing procedures to address the requirements of a cyber security training program.

Licensee/Applicant Activities

[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 to provide high assurance that these individuals are able to perform their job functions properly.

C.10.2 Awareness Training

Control Intent

The intent of this control is to ensure appropriate cyber security awareness training for all applicable personnel is defined, developed, provided, and maintained.

Pre-Decisional

Licensee/Applicant Activities

[Licensee/Applicant]'s cyber security awareness training is designed to increase an individual's sensitivity to cyber threats and vulnerabilities and his or her 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 log-on 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;
- insider threat; and
- CDAs to which personnel have authorized access

[Licensee/Applicant] establishes, implements, and documents requirements for cyber security awareness training for [Licensee/Applicant] employees and contractors that 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 central processing unit 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

Pre-Decisional

- antivirus or intrusion detection system alerts
- disabled antivirus software and other security controls
- unexpected patch changes
- machines connecting to outside IP addresses
- requests for information about the system (social engineering attempts)
- unexpected changes in configuration settings
- unexpected system shutdown
- unusual activity from control devices
- loss of signal from control devices
- unusual equipment in secure areas

- organizational contacts that should receive reports of 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

Control Intent

The intent of this control is to ensure technical and cyber security training supports the roles and responsibilities of all applicable personnel.

Licensee/Applicant Activities

[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 who have cyber security responsibilities related to programs, processes, and procedures, or individuals who 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.

- 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 that addresses the following:

Pre-Decisional

- knowledge of specific cyber security and engineering procedures, practices, and technologies, including implementation methods and design requirements, that 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

Control Intent

The intent of this control is to ensure specialized cyber security training supports the roles and responsibilities of personnel involved in the implementation of the cyber security program.

Licensee/Applicant Activities

[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 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 CSPs 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.

Pre-Decisional

C.10.5 Cross-Functional Cyber Security Team

Control Intent

The intent of this control is to ensure a cross-functional CST is established to monitor, address, and manage cyber security issues.

Licensee/Applicant Activities

[Licensee/Applicant] develops, implements, and documents a cross-functional CST.

[Licensee/Applicant] develops, implements, and documents a program to share expertise and varied domain knowledge among 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

Control Intent

The intent of this control is to ensure appropriate personnel understand plant physical processes and how any CDA's compromise may affect those processes.

Licensee/Applicant Activities

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

C.10.7 Feedback

Control Intent

The intent of this control is to ensure implementation of a feedback program to refine the cyber security program and identify training gaps.

Licensee/Applicant Activities

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

Pre-Decisional

C.10.8 Security Training Records

Control Intent

The intent of this control is to ensure individual cyber security training is documented and monitored.

Licensee/Applicant Activities

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

C.10.9 Contacts with Security Groups and Associations

Control Intent

The intent of this control is to ensure personnel receive and maintain the necessary technical skills to perform their assigned roles within the licensee's cyber security program.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure establishment of a security organization possessing the authority, technical and operational expertise, and formal responsibility for implementing, maintaining, and managing the licensee's cyber security program.

Licensee/Applicant Activities

[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:

- has 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

Pre-Decisional

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 about 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 CSP;
- 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 in the area of cyber security.

Role: Cyber Security Incident Response Team

Team Member Requirements:

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

Pre-Decisional

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

Control Intent

The intent of this control is to ensure all required configuration management security controls are established, implemented, and documented.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure development, documentation, and deployment of policies and associated implementing procedures to address the requirements of configuration management.

Licensee/Applicant Activities

[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. [Licensee/Applicant] documents and assesses changes to hardware, software, and configuration settings in accordance with these policies and implementing procedures.

The structured configuration management process evaluates and controls changes to CDAs to ensure that they remain secure. Before any change is implemented, [Licensee/Applicant] confirms that new vulnerabilities are not introduced to the CDA or to CDAs that connect to, or communicate with, the modified CDA. Approved CDA configuration changes should be associated with the documented CDA security assessment.

Pre-Decisional

[Licensee/Applicant] applies security protections throughout a CDA's life cycle—procurement and identification, initial assessment, deployment and operation, maintenance, and decommissioning.

C.11.3 Baseline Configuration

Control Intent

The intent of this control is to ensure implementation of processes and procedures to verify, maintain, and restore the approved configuration of all CDAs, mobile devices, and boundary control devices.

Licensee/Applicant Activities

[Licensee/Applicant] develops, documents, and maintains a current baseline configuration of CDAs, mobile devices, and boundary devices 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 them [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, mobile device, and boundary device, [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 following the [Licensee/Applicant] change control process.

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

[Licensee/Applicant] employs a "deny-all, permit-by-exception" authorization policy to identify and authorize software permitted on [Licensee/Applicant] CDAs, mobile devices, and boundary control devices (i.e., whitelists 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, mobile device, and boundary control device 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 prompt detection and response to intrusions;

Pre-Decisional

- 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

Control Intent

The intent of this control is to ensure all changes to CDAs are documented and authorized.

Licensee/Applicant Activities

[Licensee/Applicant] is responsible for the following:

- authorizing and documenting configuration change decisions associated with CDAs
- retaining and reviewing records of CDA configuration changes and audit activities associated with CDA configuration changes and employing [manual/automated] mechanisms to accomplish the following:
    - 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

Control Intent

The intent of this control is to ensure an impact analysis is conducted, before making any changes, to identify potential impairments to the security of the CDA.

Licensee/Applicant Activities

The [Licensee/Applicant]'s CST performs a security impact assessment before making changes to CDAs consistent with Section 4.2.2 of [this Plan (Appendix A)] 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.

Pre-Decisional

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

C.11.6 Access Restrictions for Change

Control Intent

The intent of this control is to ensure physical and logical access to implement changes to CDAs is restricted to authorized personnel only. This control also intends to ensure all changes for auditing are recorded and tested and that change records are periodically reviewed to detect unauthorized modifications.

Licensee/Applicant Activities

[Licensee/Applicant] defines, documents, approves, and enforces physical and logical access restrictions associated with changes to CDAs.

[Licensee/Applicant] generates, retains, and audits the record of these changes [quarterly] as well as 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 when 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 prompt 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.

Pre-Decisional

C.11.7 Configuration Settings

Control Intent

The intent of this control is to ensure the establishment and documentation of configuration settings for a CDA with the most restrictive mode necessary to perform its functions, based on the CDA's operating requirements.

Licensee/Applicant Activities

[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 (e.g., disable unused ports and wireless communications, software controlled operational modes, basic input-output system settings);
- documenting hardware configuration settings pertaining to operational functionality (e.g., switches, jumpers, shunts);
- documenting and approving any deviations 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/manual mechanisms] to respond to unauthorized changes to [Licensee/Applicant]-defined configuration settings; and
- documenting the justification for alternate (compensating) security controls when 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 prompt 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;

Pre-Decisional

- 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

Control Intent

The intent of this control is to ensure CDAs have no unnecessary applications, functions, utilities, services, communication capabilities, interfaces, or peripherals beyond those needed for SSEP functions.

Licensee/Applicant Activities

[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 disable unnecessary or nonsecure functions, ports, protocols, and services. [Licensee/Applicant] documents and employs automated mechanisms to prevent unauthorized program execution. [Licensee/Applicant] uses [whitelists, blacklists, graylists] application control technologies.

C.11.9 Component Inventory

Control Intent

The intent of this control is to ensure that an up-to-date inventory for CDAs and their constituent parts is developed, documented, and maintained.

Licensee/Applicant Activities

[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;

Pre-Decisional

- employs automated mechanisms to detect the presence or addition of unauthorized hardware, software, and firmware components or devices and disables access by such components or devices (i.e., disables network access, isolates the component) 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

Control Intent

The intent of this control is to ensure the development, documentation, and deployment of policies and procedures to address requirements for the acquisition of systems, devices, and services.

Licensee/Applicant Activities

[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

Control Intent

The intent of this control is to ensure items and services are procured from trusted sources and have traceability though use of a trusted distribution path.

Licensee/Applicant Activities

[Licensee/Applicant] protects against supply chain threats and vulnerability by employing the following measures to maintain the integrity of the CDAs that are acquired:

- establishing trusted distribution paths;
- validating vendors; and
- requiring tamper-proof products, tamper-evident seals, or integrity checking mechanisms on acquired products.

Pre-Decisional

[Licensee/Applicant] conducts an analysis for each product acquisition to determine that the product provides the security requirements necessary to address the security controls in Appendices 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

Control Intent

The intent of this control is to ensure acquired or developed software is free from known cyber security vulnerabilities, as well as unauthorized and undocumented functionality and features.

Licensee/Applicant Activities

[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 that all tools used to perform cyber security tasks or SSEP functions 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

Control Intent

The intent of this control is to ensure that guidelines for the integration of security capabilities into organizational acquisitions are established.

Licensee/Applicant Activities

[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;
- promptly conducting analyses by identifying, evaluating, and documenting the effects that each advancement could have on the security, safety, and operation of critical assets, systems, CDAs, and networks and implementing these advancements; and
- replacing legacy systems as they reach the end of life with systems that incorporate security capabilities.

Pre-Decisional

[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 and Evaluation

Control Intent

The intent of this control is to ensure that licensees establish procurement language that requires system developers and integrators of acquired software-based CDAs to have an effective and properly managed software assurance program.

Licensee/Applicant Activities

[Licensee/Applicant] documents and requires that system developers and integrators of acquired CDAs create, implement, and document a security assessment plan to ensure that the acquired products meet all specified security requirements including the following:

- the products are free from known, testable vulnerabilities and malicious code and
- the 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 developers and integrators to produce evidence of the execution of the security assessment plan and results of security testing and evaluation.

[Licensee/Applicant] requires the developer to ensure 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 demonstrate that they are effective, in accordance with Section A.4.1.2 of [this Plan (Appendix A)].

[Licensee/Applicant] requires the developer to perform and document attack surface reviews to analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of those changes.

C.12.6 Licensee/Applicant Testing

Control Intent

The intent of this control is to ensure that CDAs are tested for vulnerabilities and effective security controls before introduction into a production environment or network, and throughout the CDAs' life cycle.

Licensee/Applicant Activities

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

[Licensee/Applicant] is responsible for the following:

Pre-Decisional

- 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;

- implementing the security controls in Appendices B and C to RG 5.71 in accordance with the process described in Section 3.1.6 of [this Plan (Appendix A)];

- testing the security controls for effectiveness, as described in Section 4.1.2 of [this Plan (Appendix A)], and the performance of vulnerability scans, in accordance with Section 4.1.3 of [this Plan (Appendix A)] and Section 13.1 of this plan, against the CDA in its integrated state and correction, elimination, or discussion of discovered vulnerabilities;

- installing and testing the CDA in the target environment;

- conducting attack surface reviews to analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of those changes; and

- conducting an acceptance review and test of the CDA security features.

[Licensee/Applicant] documents the following:

- Security controls are implemented in accordance with Appendix B to RG 5.71.

- The effectiveness of the security controls implemented in accordance with Appendix C is verified.

- Security design features are 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 RG 5.7.1. For each security feature or configuration to be implemented, the documentation describes the feature, its method of implementation, and any configurable options associated with the feature. Each security feature designed into the system is traceable to its corresponding security requirement.

- Attack surface reviews and mitigations to address attack vectors generated as a result of design and implementation changes are documented.

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.

Pre-Decisional

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

- 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

Control Intent

The intent of this control is to ensure the technical and operational elements of the licensee's defensive strategy are sufficiently protected against known threats, vulnerabilities, and attack methods.

Licensee/Applicant Activities

[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 [this Plan (Appendix A)] 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 accomplishing the following:

    - enumerating platforms, software flaws, and improper configurations
    - formatting and making transparent checklists and test procedures
    - 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 mechanisms that include the capability to update the list of known vulnerabilities;

- update the list of vulnerabilities associated with the CDA scanned [monthly] and when new vulnerabilities are identified and reported;

Pre-Decisional

- 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, using methods such as [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 scanning is 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 whether a vulnerability identified in the CDA has been previously exploited.

C.13.2 Risk Mitigation

Control Intent

The intent of this control is to ensure a CSP has been implemented and its protective measures are in place, operating as intended, and producing desired outcomes.

Licensee/Applicant Activities

Protection and mitigation of risk are achieved by implementing (1) the defense-in-depth protective strategies discussed in Section 3.2 of RG 5.71, (2) the security controls described in Appendices B and C to RG 5.71, (3) digital equipment and software cyber attack detection, prevention, and recovery techniques and tools for the systems, structures, and components within the scope of the rule, and (4) Section 4 of [this Plan (Appendix A)]. [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.

Pre-Decisional

C.13.3 Corrective Action Program

Control Intent

The intent of this control is to ensure cyber security issues and deficiencies, particularly those identified as the result of a cyber security inspection or incident, are documented, addressed, managed, and promptly and appropriately corrected.

Licensee/Applicant Activities

[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.

Pre-Decisional