United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-7141

The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors

Office of Nuclear Security and Incident Response

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:
Address: U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: DISTRIBUTION.RESOURCE@NRC.GOV
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—
The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—
American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

DISCLAIMER: This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-7141

The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors

Manuscript Completed: September 2014
Date Published: November 2014

Prepared by
C. Chenoweth
J. Green
T. Shaw
M. Shinn
G. Simonds

MAR, Incorporated
1803 Research Boulevard
Suite #204
Rockville, MD 20850-6106

Jonah Pezeshki, Security Specialist (Cyber)

Office of Nuclear Security and Incident Response

ABSTRACT

This report, NUREG/CR-7141, “the U.S. NRC Cyber Security Regulatory Framework for Nuclear Power Reactors” is a knowledge management product that provides an overview of, and historic perspective of the development of Regulatory Guide (RG) 5.71, “Cyber Security Programs for Nuclear Facilities.” Further, this report provides a comparative analysis between the programmatic guidance contained within RG 5.71 and both the National Institute of Standards and Technology (NIST) Risk Management Framework found in NIST Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems,” Revision 1, and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. This framework correlates the high baseline security controls published by NIST in Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations,” Revision 3, to those contained in Appendices B and C of RG 5.71 (“Technical Security Controls” and “Operational and Management Security Controls”, respectively). This report is not regulatory guidance and does not supersede policy decisions made by the NRC on behalf of security programs defined in the NRC’s regulations, or rules. Nor does this report impose any new requirements or interpretations of NRC regulations that could be used for complying with a license’s approved cyber security plan, as defined in Title 10 of the Code of Federal Regulations (CFR) Part 73.54, “Protection of Digital Computer and Communication Systems and Networks” (10 CFR 73.54).

CONTENTS

ABSTRACT iii
CONTENTS v
ACRONYMS vii

1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
1.3 Background 2

2 NRC CYBER SECURITY REGULATORY FRAMEWORK FOR NUCLEAR FACILITIES 5
2.1 NRC Cyber Security Controls 8
2.2 NRC Cyber Security Regulatory Framework and the NIST Risk Management Framework (RMF) 10

3 FINAL CONSIDERATIONS 15

APPENDIX A: NIST SECURITY CONTROLS FULLY ADDRESSED BY NRC REGULATORY FRAMEWORK A-1

APPENDIX B: PARTIALLY MATCHED NIST AND NRC SECURITY CONTROLS B-1

APPENDIX C: NON-MATCHING NIST AND NRC SECURITY CONTROLS C-1

APPENDIX D: SECURITY CONTROLS UNIQUE TO NRC D-1

APPENDIX E: COMPARISON BETWEEN RG 5.71 SECURITY CONTROLS AND NERC CIP (UPDATED MARCH, 2012) STANDARDS E-1

APPENDIX F: LOCATION OF REFERENCED DOCUMENTS F-1

ACRONYMS

BIOS	Basic Input Output System
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CM	Continuous Monitoring
CS	Critical System
CSIR	Cyber Security Incident Response
CSIRT	Cyber Security Incident Response Team
CSP	Cyber Security Plan
CST	Cyber/Computer Security Team
DHS	Department of Homeland Security
DoD	U.S. Department of Defense
ERDS	Emergency Response Data System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
I&C	Instrumentation and Control
ICS	Industrial Control System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISA	International Society of Automation
IT	Information Technology
MOA	Memorandum of Agreement
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
NSIR	Nuclear Security and Incident Response
RG	Regulatory Guide
RMF	Risk Management Framework
SGI	Safeguards Information
SP	Special Publication
SSEP	Safety, Security, and Emergency Preparedness

1 INTRODUCTION

1.1 Purpose

The purpose of this report is to provide information and background regarding the programmatic approach taken by the U.S. Nuclear Regulatory Commission (NRC) in developing its cyber security regulatory framework, and an overview of the considerations made by the NRC when developing cyber security controls to protect critical systems and equipment at licensed commercial nuclear power reactors from cyber-based attacks. The NRC's cyber security regulatory framework includes cyber security regulation, regulatory guidance, and licensing and oversight activities. In addition, this report provides a correlation between the NRC's cyber security controls and the March 2012 version of North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards.

1.2 Scope

The scope of this document covers the following:

- an overview of the NRC cyber security regulatory framework
- a comparison of the programmatic guidance contained in Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," Revision 0, (RG 5.71) with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) described in NIST Special Publication (SP) 800-37, Revision 1, (NIST RMF)
- the tailoring of protective measures (security controls) for use by nuclear power reactors that are flexible, scalable, effective, and verifiable
- a comparison of security controls in RG 5.71 and NERC CIP standards

The NRC cyber security regulatory framework is one part of many regulations governing safety and security at nuclear power reactors. It is important to understand the consideration of other NRC regulatory programs in the development of the cyber security regulatory framework for nuclear power reactors. This is essential to effectively understanding the comparison of the high baseline security controls contained in the NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3, (NIST SP 800-53) with those found in RG 5.71, because many of the NIST security controls are addressed through a variety of NRC regulations and associated requirements. Sections 3 and 4 of this report provide additional context in this regard.

Section 5 details the process used to develop NRC's security controls. Section 6 provides a brief comparison of the NRC's cyber security regulatory framework to the NIST RMF. In addition, Section 7 provides an overview of the regulatory responsibilities coordinated between NERC and the NRC as part of a memorandum of agreement (MOA) that acknowledges agreed upon roles and responsibilities for regulatory oversight of cyber security at nuclear power reactors.

Appendix A provides a mapping of NIST high baseline security controls to NRC security controls, regulatory requirements, and programmatic provisions in the applicants' and licensees' NRC-approved cyber security plans. Because of the tailoring process, in some cases the NRC security controls partially address all the elements contained within the NIST security controls. More information on partially matched security controls is discussed in Appendix B. Appendix C outlines those NIST security controls for which there are no corresponding NRC security controls. Security controls that are unique to NRC are presented in Appendix D. Appendix E

compares the suite of NRC security controls in RG 5.71 with the March 2012 version of NERC's CIP reliability standards.

This report is not regulatory guidance and does not supersede policy decisions made by the NRC on behalf of security programs defined in the NRC's regulations, or rules. Nor does this report impose any new requirements or interpretations of NRC regulations that could be used for complying with a license's approved cyber security plan, as defined in Title 10 of the Code of Federal Regulations (CFR) Part 73.54, "Protection of Digital Computer and Communication Systems and Networks" (10 CFR 73.54).

1.3 Background

The NRC's regulations are developed and amended through the rulemaking process, which includes public review and comment. Through licensing, the NRC grants an individual or entity, hereafter referred to as "licensee," authorization to conduct regulated activities, including operating a nuclear power reactor.

Once a license is issued, the NRC performs oversight of licensee activities in the form of on-site inspections, performance assessments, investigations of wrongdoing, and formal sanctions in cases where there was determined to be a violation of NRC regulation.

Following the events of September 11, 2001, the NRC underwent a comprehensive review of the security requirements and potential vulnerabilities at regulated nuclear facilities. The NRC issued security orders[1] to expeditiously impose requirements to enhance security (including consideration of cyber security) above what was already required by existing regulations. Orders issued in 2002 and 2003[2] contained requirements for licensees to implement interim compensatory measures for both physical and cyber-based security, and added cyber-based attacks as a characteristic of the design basis threat. The design basis threat is a profile used to define the type, composition, and capabilities of a threat actor, or adversary, that commercial nuclear power reactors must defend against to prevent acts of radiological sabotage. Subsequent actions taken by the NRC to address cyber-based threats included the following:

- 2004 – Publication of NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," October 2004, providing guidance on methods for conducting cyber security self-assessments

- 2005 – NRC endorsement of the Nuclear Energy Institute (NEI) 04-04, "Cyber Security Program for Power Reactors," providing guidance for developing and maintaining a cyber security program at licensed nuclear utilities

- 2006 – Publication of NRC RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 2006, providing guidance for the

[1] The NRC issues security orders to require licensees to implement security measures beyond those required by NRC regulations at the time and as conditions of issued licenses when necessary for adequate protection of public health and safety or common defense and security. Orders can be used to modify, suspend, or revoke licenses or require specific actions by licensees or other persons. Orders can also be used to impose civil penalties.

[2] NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," February 2002, and NRC Order EA-03-086, "Design Basis Threat for Radiological Sabotage," April 2003.

secure design, development, and implementation of safety related digital instrumentation and control systems

- 2007 – Publication of Branch Technical Position 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” March 2007, stating that system cyber security features be maintained under a configuration management program, tested, and that safety analysis includes consideration of cyber security risks

- 2010 – NRC endorsement of the Nuclear Energy Institute (NEI) 08-09, “Cyber Security Plan for Nuclear Power Reactors,” which was developed by NEI to assist licensees in complying with the requirements of 10 CFR 73.54

- 2013 – NRC endorsement of the Nuclear Energy Institute (NEI) 13-10, “Cyber Security Control Assessments,” which was developed by NEI to provide guidance for implementing a consequence-based approach to the implementation of cyber security controls for a licensee’s Critical Digital Assets (CDAs); the consequence-based approach described in this document will likely be incorporated into a future revision of RG 5.71

In 2005, the NRC began the rulemaking process to revise its regulations to include requirements contained in the aforementioned security orders. In 2009, the NRC finalized its rulemaking effort and issued new cyber security regulation (i.e., 10 CFR 73.54) for nuclear power reactors, hereafter referred to as the cyber security regulation. The cyber security regulation requires that a licensee’s cyber security program be incorporated as a component of the on-site physical protection program. As such, the cyber security plan is one of four security plans described in 10 CFR Part 73.55, “Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.” Collectively these plans outline how a facility will establish and maintain an on-site security organization (physical security plan), train and qualify security personnel (training and qualification plan), implement predetermined response plans and strategies (safeguards contingency plan), and protect CDAs from cyber-based attacks (cyber security plan). Once approved by the NRC, these plans are incorporated into the facility’s license and are subject to NRC oversight.

At the time the NRC published RG 5.71, the Federal Energy Regulatory Commission (FERC) had recently issued Order 706, requiring critical infrastructure protection (CIP) standards to protect bulk electric systems. However, the Order included a provision that exempted facilities regulated by the NRC. This created a gap between the NRC’s oversight and NERC’s oversight that resulted in the two agencies coordinating between the NRC’s task in protecting safety, security, and emergency preparedness systems against radiological sabotage, and NERC’s focus on structures, systems, and components (SSCs) in the plant relied upon to maintain continuity of the bulk electric systems. This gap was later addressed by FERC, via Order 706-B. However, this new order instead created potential overlap between the regulatory coverage by NRC and FERC. Subsequently, a memorandum of agreement was reached between FERC and the NRC to include balance of plant SSC’s into the NRC’s regulatory framework as important to safety. Appendix E of this report therefore correlates the NRC’s cyber security controls, including existing regulatory framework in safety, security, and emergency preparedness, with NERC's CIP reliability standards at the time RG 5.71 was published.

2 NRC CYBER SECURITY REGULATORY FRAMEWORK FOR NUCLEAR FACILITIES

The NRC's cyber security regulation requires nuclear power reactors to develop, implement, and maintain an on-site cyber security program. The regulation focuses on the protection of digital assets from cyber-based attacks that could adversely impact safety, important-to-safety, security, and emergency preparedness functions at a nuclear power plant. The NRC's cyber security regulation is performance-based, which the NRC defines as the following:

> Performance-based regulation leads to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives for licensees to improve safety without formal regulatory intervention by the agency.

As part of the performance requirement, the cyber security regulation requires new and operating nuclear power reactor applicants and licensees to submit their respective cyber security plans to the NRC for review and approval. The cyber security plan must describe how the applicant or licensee will meet the regulation with consideration of site-specific conditions that could affect implementation of the approved plan. In addition, the cyber security regulation requires that the cyber security program protect digital computers, communication systems, and networks associated with critical plant functions from cyber-based attacks. To meet that objective, the cyber security plan includes performance-based requirements for the following:

- ensuring that critical plant functions are not adversely impacted by a cyber-based attack
- conducting analyses to determine which digital assets at the plant require protection, referred to as critical digital assets (CDAs), and implementing security controls to protect these digital assets
- applying and maintaining defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber-based attacks, such as the following:
    - prompt detection and response to cyber-based attacks
    - mitigating the adverse impacts and consequences of cyber-based attacks
    - correcting exploited vulnerabilities
    - restoring CDAs affected by a cyber-based attack
- conducting cyber security awareness training for appropriate facility personnel and contractors
- evaluating and managing cyber risks
- conducting cyber security evaluations for asset modifications
- developing and maintaining written documentation and procedures for cyber security plan implementation
- incorporating the cyber security program as a component of the plant's physical protection program

RG 5.71 provides guidance on an acceptable approach to satisfy the requirements of the NRC's cyber security regulation and details an acceptable method for licensees and applicants to establish cyber security programs. RG 5.71 also promotes the use of a multi-level defensive strategy and outlines other important considerations that should be part of a comprehensive cyber security program. Appendix A of RG 5.71 includes a cyber security plan template that applicants and licensees can use and modify as necessary to account for site specific conditions. Provisions in the cyber security plan that are referenced in the appendices of this report are denoted by section number from Appendix A of RG 5.71 (e.g., A.3.1.2 Cyber Security Team).

In developing RG 5.71, the NRC considered publications from several standards organizations, such as the International Society of Automation (ISA), the Institute of Electrical and Electronics Engineers (IEEE), and NIST, as well as guidance from the Department of Homeland Security (DHS). In addition, RG 5.71 describes a protection strategy from cyber-based attacks that consists of a defensive architecture and a set of tailored security controls based on NIST SP 800-53 and NIST SP 800-82, "Guide to Industrial Control Systems Security." Figure 1 below provides an overview of the security lifecycle process described in RG 5.71.

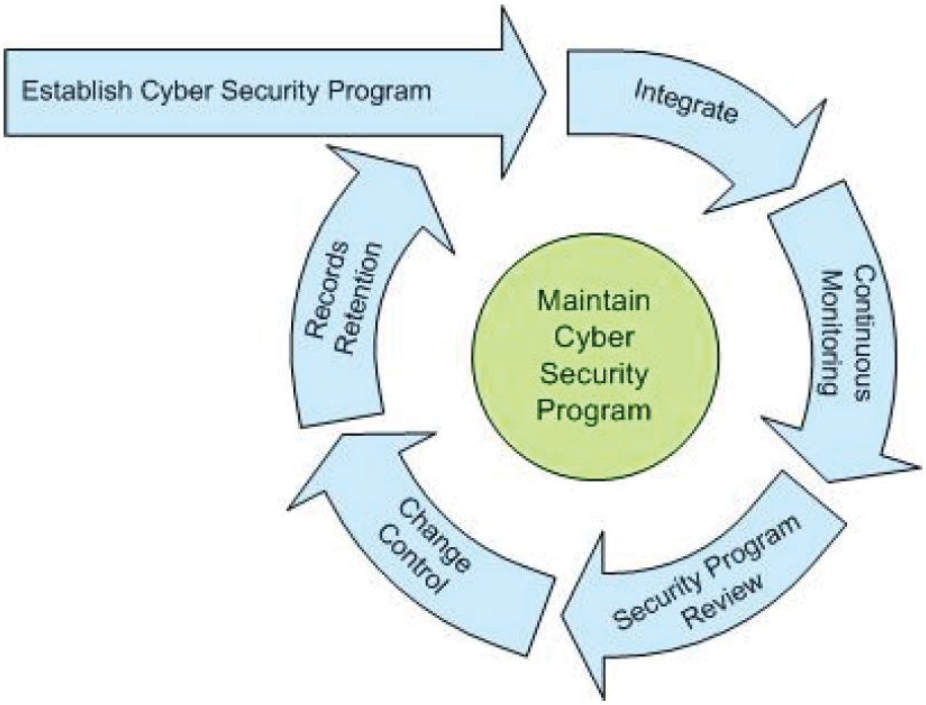

Figure 1: RG 5.71 Security Lifecycle

Establishing, implementing, and maintaining the cyber security program is accomplished by using formal assessment methods carried out by qualified staff at nuclear power reactors acting under the authority of the site's approved policy and the supervision of senior site management. Determining which digital assets at the plant require protection from cyber-based attacks hinges on the involvement of a multi-disciplinary team of site personnel that possess broad knowledge and expertise in a variety of areas, such as information technologies, plant operations, engineering, safety, physical security, and emergency preparedness.

The on-site team documents its analysis for each digital asset that requires protection (i.e., CDA identification) and conducts validation reviews of direct and indirect connectivity pathways, physical location, configurations, interdependencies with other digital assets, the effectiveness of any security controls that are in place and the location of the CDA within the facility's defensive architecture.

Establishing a site-specific cyber security program at a nuclear power reactor also entails addressing potential cyber risks for CDAs through the implementation of management, operational, and technical cyber security controls. To maximize program effectiveness, the cyber security program is incorporated into the site's physical protection program. This promotes the coordination and the integration of security tasks across the facility to better leverage the protective measures offered by each program to meet the performance-based regulatory requirements for defending against the design basis threat.

The NRC cyber security regulatory framework for nuclear power reactors also promotes the evaluation and management of cyber security risk through continuous monitoring, cyber security program reviews, change control, and records retention. Though represented sequentially in Figure 1 above, these steps may also take place as parallel activities. Continuous monitoring involves the ongoing assessment of security controls by site personnel to ensure that measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements defined within the control. This includes the need for site personnel to perform vulnerability scans and assessments, and to measure security control effectiveness, to fully assess, address and remediate known security threats and vulnerabilities. Furthermore, program-level effectiveness reviews are performed at nuclear power reactors using site-specific analysis and assessments to determine if the security measures in place to protect CDAs are sufficient to meet the requirements of the cyber security regulation and license conditions set forth in the facility's NRC-approved cyber security plan. The primary objective of the NRC-approved security plan is to provide the means to implement sufficient controls to prevent the following adverse impacts on critical plant functions:

- the compromise of integrity or confidentiality of software and/or data
- the intentional or accidental denial of authorized access to systems, services, and/or data
- the disruption of systems, networks, and associated equipment operation

Any deficiencies identified during continuous monitoring or security program reviews are documented and tracked within the licensee's corrective action program, which is designed to capture issues related to adverse conditions at the plant and ensure that performance deficiencies are promptly identified and corrected.

In the next step of the security lifecycle, changes or modifications are coordinated and controlled to ensure each CDA's security posture is not degraded. This is accomplished by systematically planning, approving, testing, and documenting changes to the environment wherein the CDA resides or operates, or the changes to the CDA itself. Change control is heavily reliant on good configuration management practices. This may, for example, include having sound policies and procedures in place governing configuration management for CDAs, component inventory, documenting each CDAs baseline configuration, authorizing changes to CDAs before modifications are applied, restricting who can perform modifications, and conducting a security impact analysis before and after each modification to ensure the security posture of a CDA was not adversely impacted. Change control may also involve evaluating the

operational requirements of each CDA to document, configure, and enforce the most restrictive operational settings and ensure configuration settings are (1) limited to essential capabilities only and (2) insecure functions, ports, protocols, and services are prohibited, protected, or removed.

All records and documentation, developed as part of the licensee's cyber security program, are maintained at the site. Records retention is important for capturing historical data that may be useful later in conducting after-the-fact investigations, forensics analysis, and administering evidence pertaining to security-related incidents.

2.1 NRC Cyber Security Controls

The NRC suite of security controls (presented in Appendices B and C of RG 5.71) was derived primarily from the high baseline security controls in NIST SP 800-53. The high baseline is one of three baselines of security controls used by NIST to assist organizations, particularly Federal agencies, in applying appropriate security categorizations to information systems and a corresponding suite of security controls that is commensurate with security objectives of confidentiality, integrity, and availability. NRC cyber security controls referenced in the appendices of this report are denoted by section numbers from Appendices B and C of RG 5.71 (e.g., B.3.8 Trusted Path).

RG 5.71 was initially under development in late 2008, during which the NIST SP 800-53 and NIST SP 800-82 were out for public comment and not yet finalized. By August of 2009, the NIST SP 800-53, was completed and included an appendix that provided guidance on the unique characteristics of Industrial Control Systems (ICS) and recommendations for the customization of security controls for use with these technologies. DHS published its "Catalog of Control Systems Security: Recommendations for Standards Developers" in September of 2009 as well, which provided a compilation of ICS security controls and practices. The DHS guidance noted that "various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks." The NIST SP 800-82, however, would not be completed until later in June of 2011.

By relying on the NIST SP 800-53, catalog of security controls and ICS security guidance available at the time, the NRC developed a standards-based set of tailored, or modified, cyber security controls that align with its regulatory framework and the unique operating environments at nuclear power reactors. To accomplish this, the NRC followed the suggestion provided by NIST in Appendix I, "Industrial Control Systems," of NIST SP 800-53, to tailor security controls according to ICS-specific needs and requirements. Analyses considering the NRC's regulatory framework were performed by digital instrumentation and control (DI&C) and plant operations experts from the NRC, the commercial nuclear power industry and the private sector for each NIST SP 800-53, high baseline security control. The purpose of these analyses was to determine which security controls (1) could be implemented with little to no modification, (2) were already addressed by an existing NRC regulation or other regulatory commitments, (3) required modification to be applicable to operational and environmental conditions at nuclear power reactors, or (4) were deemed not applicable because they could not be implemented as written on CDAs in use at nuclear power reactors or pertained to activities that were outside the NRC's regulatory jurisdiction.

The principle safety and security regulations that were used in tailoring decisions of the NIST SP 800-53, Revision 3, when developing the NRC suite of cyber security controls in RG 5.71, include the following:

10 CFR Part 26, “Fitness for Duty Programs”

- Fitness for Duty (FFD) requirements for individuals working at power reactors, including training, drug and alcohol testing, behavioral observation, and employee assistance programs

10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities”

- addresses licensing conditions for the safe operation (e.g., certifications, codes of standards, enforcement, design criteria) of nuclear power reactors

10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants”

- addresses the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power reactors

10 CFR Part 73, “Physical Protection of Plants and Materials

- addresses the vast majority of regulatory security requirements, including both physical and cyber security, for example the following:
    - 10 CFR Part 73.1, “Purpose and scope” addresses requirements for the establishment and maintenance of a physical protection system for the protection against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material
    - 10 CFR Part 73.54, “Protection of digital computer and communication systems and networks” addresses implementation of a cyber security program at nuclear power reactors to provide high assurance that digital computer and communication systems and networks associated with crucial plant functions are adequately protected against cyber-based attacks, up to and including the design basis threat as described in 10 CFR Part 73.1
    - 10 CFR Part 73.55, “Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage” addresses implementation of a physical protection program at nuclear power reactors to provide high assurance that activities involving special nuclear material are not inimical to common defense and security and do not constitute an unreasonable risk to the public health and safety
    - 10 CFR Part 73.56, “Personnel access authorization requirements for nuclear power plants” addresses measures to ensure individuals granted unescorted access to nuclear power reactors are trustworthy and reliable, so that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage
    - 10 CFR Part 73.58, “Safety/security interface requirements for nuclear power reactors” addresses measures to resolve potential conflicts with the implementation of safety and security measures at nuclear power reactors by taking compensatory and/or mitigating actions, when necessary, to maintain compliance with safety and security regulations, requirements, and license conditions

10 CFR Part 100

- addresses site requirements that must be satisfied or considered during development of emergency plans at nuclear power and test reactor facilities

2.2 NRC Cyber Security Regulatory Framework and the NIST Risk Management Framework (RMF)

When developing its cyber security regulatory framework, the NRC considered and relied upon the NIST RMF, by incorporating a structured but flexible lifecycle methodology for cyber security controls and encourages organizations to perform the following:

- incorporate security strategies consistently and comprehensively throughout their digital-based operations

- assign responsibility at the senior levels of corporate and site management for the identification and mitigation of system related security risks

- integrate risk management principles into the enterprise architecture and throughout the asset acquisition and implementation process (including procurement, development, testing and deployment, and maintenance phases)

- conduct ongoing risk assessments and continuous monitoring of the effectiveness of the implemented security controls

These attributes of the RMF align with performance requirements set forth in NRC cyber security regulation 10 CFR Part 73.54, RG 5.71, and provisions outlined in licensee cyber security plans. A key facet of the RMF is the emphasis on a disciplined risk identification and mitigation process, while accommodating flexibility in how risk mitigation strategies are implemented. This aspect of the RMF approach is similar to the performance-based NRC cyber security regulatory framework, in that the cyber security regulation, RG 5.71 and cyber security plans, were designed to offer flexibility in how nuclear power reactors implement their site-specific, comprehensive cyber security programs that ensure CDAs associated with critical plant functions are protected from cyber-based attacks.

The NIST RMF is composed of six phases and aims to support Federal agencies in managing risk in the design, development, implementation, operation, maintenance, and disposition of Federal information systems. Figure 2 below illustrates the six phases of the RMF:

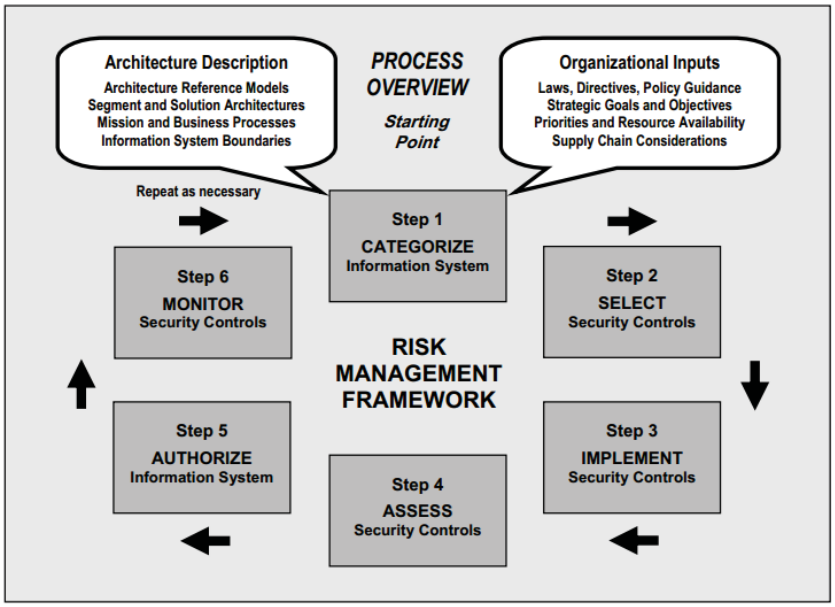

Figure 2: NIST Risk Management Framework

When comparing the RMF to the NRC cyber security regulatory framework, several factors are important to understand. For example, CDAs (including computers, communications systems, and networks) in use at nuclear power reactors are not federally owned and operated. With few exceptions, [3] these CDAs are owned by organizations in the private sector and are not managed by federal employees. In addition, the term "risk management" is applied differently. Within the RMF, risk management is a process of managing risk through a combination of assessments, mitigation strategies, and continuous monitoring activities that focus primarily on impact and likelihood measurements. For example, this process is accomplished by assessing the impact of a threat actor exploiting a vulnerability on a CDA, the likelihood of that event occurring, mitigation strategies to reduce the event impact, or its likelihood, and by performing ongoing reviews to ensure that applied mitigation strategies remain effective. In addition, there are provisions for assessing the impact that a cyber-based attack would have on CDAs associated with critical plant functions, such as denying access to systems, services, or data; adversely impacting the confidentiality and integrity of data and/or software; and adversely impacting the operation of systems, networks, and associated equipment. If site-specific analysis demonstrates that these impacts exist, mitigation strategies defined in the cyber security plan must be implemented to provide high assurance that these assets are protected from cyber-based attacks, which is a capability of the design basis threat.

Unlike the RMF, however, there are also no provisions in NRC regulation or guidance for licensee consideration of the likelihood of a cyber event when determining risks at the facility. The NRC's performance-based regulations require that licensees ensure the capabilities to detect, assess, interdict, and neutralize threats from the design basis threat are maintained at all times. Though it may be revisited in future revisions, RG 5.71 currently states that regardless of what mitigation strategy a licensee decides to implement when addressing security controls for a CDA, the outcome must be that threat and attack vectors associated with the corresponding security control(s) are "eliminated or mitigated." Furthermore, the characteristics and attributes of the design basis threat are established and defined by the NRC through regulation 10 CFR

[3] The Tennessee Valley Authority is a corporation of the U.S. government and licensed by the NRC for operation of the Browns Ferry, Sequoyah, and Watts Bar Nuclear Power Plants.

73.1. Therefore, an assessment of the likelihood of an event occurring at a nuclear power reactor is not an industry-level activity.

Further, unlike the RMF which allows senior leaders within an organization the ability to make decisions on accepting cyber-related risks, no such provision exists under NRC regulations except under extraordinary circumstances. Under emergency conditions, a qualified senior leader at the facility can suspend a security measure when the suspension is immediately needed to protect the public health and safety. However, during non-emergency conditions, decisions on the acceptability of cyber risk are negated by the requirement to maintain protection at all times. A comparative overview of the NIST RMF steps and NRC cyber security regulatory programs is provided in Table 1 below.

More recently, in 2013, the NRC endorsed the Nuclear Energy Institute (NEI) 13-10, "Cyber Security Control Assessments." This document was developed to provide guidance for implementing a consequence-based approach to the implementation of cyber security controls for a licensee's Critical Digital Assets (CDAs). This allows for different CDAs to be afforded varying levels of protection, depending on the overall impact that a cyber compromise of that CDA would have on SSEP functions. This consequence-based approach will likely be incorporated into a future revision of RG 5.71.

Table 1: Comparative Review of NIST RMF and NRC Cyber Security Regulatory Framework

NIST RMF Step	RMF Step Description	NRC Cyber Security Regulatory Framework
Step 1: Categorize Information System	Security impact analysis of the information system and the information processed, stored, and transmitted by that system.	The compromise of confidentiality, integrity, and availability of CDAs associated with critical plant functions (e.g., safety, security, emergency preparedness) could result in radiological sabotage.
Step 2: Select Security Controls	Initial set of baseline security controls for the information system based on the security categorization, followed by tailoring and supplementing the baseline as needed according to assessments of organizational risk and local conditions.	The NRC selected the NIST SP 800-53, high security control baseline as the starting point for developing its suite of security controls provided in RG 5.71, Appendices B and C. The NRC tailored the NIST SP 800-53, high security control baseline as described in Section 5 of this report.

NIST RMF Step	RMF Step Description	NRC Cyber Security Regulatory Framework
Step 3: Implement Security Controls	The employment of the controls within the information system and its environment of operation.	Each licensee's or applicant's NRC-approved cyber security plan requires that all security controls be addressed for CDAs associated with critical plant functions that require protection from cyber-based attacks. This includes implementing the security control as written, implementing an alternative control that provides equal or greater protection as the original corresponding security control, or demonstrating that the security control is not applicable by justifying that the attack vector and/or pathways do not exist. Security controls are not applied if there would be an adverse impact on critical plant functions. If so, an alternative control of equal or greater protection would need to be implemented. Additional security controls or measures may be necessary if effectiveness or vulnerability analyses identify security-related gaps in a facility's cyber security program or CDA that are not covered by an existing security control.
Step 4: Assess Security Controls	Determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Qualified assessment teams verify the effectiveness of security controls and that there is high assurance that CDAs are adequately protected from cyber-based attack, up to and including the design basis threat. Independent inspection of the site-specific cyber security program and associated security control implementations will be conducted by the NRC, and any performance deficiencies subject to regulatory enforcement.
Step 5: Authorize Information System	Determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.	Decisions on the acceptability of cyber risk would be subject to regulatory review through NRC's licensing and oversight programs for determination of risk to public health and safety, common defense, and the environment.

NIST RMF Step	RMF Step Description	NRC Cyber Security Regulatory Framework
Step 6: Monitor Security Control	Ongoing assessment of security control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.	Provisions within the facility's NRC-approved cyber security plan include measures defined in this RMF step, in addition to independent NRC inspections that typically occur at least every 36 months.

3 FINAL CONSIDERATIONS

What makes the NRC cyber security regulatory framework unique is that it represents the integration of cyber security with the needs and requirements of nuclear facilities within the United States. This integration of cyber security tailors NIST cyber security standards and guidelines according to the breadth and scope of NRC regulations governing safety, security, and emergency preparedness at nuclear power reactors that are subject to regulatory oversight. As a result, the consolidated framework provides high assurance in protecting the public health and safety and promotes effective cyber security practices in the nuclear sector from the adverse consequence of cyber-based attacks.

While other sectors within the nation's critical infrastructure may find the recommendations and provisions of NRC's RG 5.71 helpful in establishing effective cyber security programs for ICS, this report demonstrates the influence of specific regulations and guidance within the nuclear sector in development of the guidance that should also be taken into consideration. Understanding the full measure of NRC's cyber security regulatory framework, therefore, requires a broader awareness of contributing regulations and programs that may not be directly referenced in RG 5.71, but were important factors in the tailoring process that led to its publication. As a result, this report may prove a helpful companion when reviewing Appendices B and C in RG 5.71, and in becoming more familiar with how the NRC is collectively addressing cyber security for nuclear power reactors.

APPENDIX A: NIST SECURITY CONTROLS FULLY ADDRESSED BY NRC REGULATORY FRAMEWORK

This appendix outlines the combination of NRC security controls, NRC regulations, and/or NRC-approved cyber security plan (CSP) commitments that provide, at a minimum, equal protections as corresponding NIST security controls. Many of the NRC security controls in this table have minor differences with their NIST counterparts, and the differences are noted.

The nomenclature convention used is the same used in Regulatory Guide 5.71. NRC security controls start with a "B" or "C" (e.g., B.1.1 – Access Control Policy and Procedures, C.1.1 – Media Protection Policy and Procedures), depending on whether the security control is a technical security control, or an operational or management security control, respectively. CSP commitments start with an "A" and correspond to the cyber security plan template sections in Appendix A of Regulatory Guide 5.71. Where more than one security control is listed, the first security control listed in the NRC Regulatory Framework is typically the primary means of addressing the NIST security control. In some cases, the NIST security control is addressed by a combination of NRC security controls, regulations, and cyber security plan commitments.

NIST 800-53 Rev 3 Controls	NRC Regulatory Framework
Control Family: Access Control	
AC-1: Access Control Policy and Procedures	B.1.1 – Access Control Policy and Procedures
AC-2: Account Management	10 CFR 73.55 10 CFR 73.56 B.1.2 – Account Management B.4.1 - Identification and Authentication Policies and Procedures C.2.2 - Personnel Termination or Transfer
AC-3: Access Enforcement	B.1.3 – Access Enforcement C.5.5 – Physical Access Control C.5.8 – Monitoring Physical Access
AC-4: Information Flow Enforcement	B.1.4 – Information Flow Enforcement
AC-5: Separation of Duties	B.1.5 – Separation of Functions
AC-6: Least Privilege	B.1.6 – Least Privilege
AC-7: Unsuccessful Login Attempts	B.1.7 – Unsuccessful Login Attempts
AC-8: System Use Notification	B.1.8 – System Use Notification
AC-11: Session Lock	B.1.10 – Session Lock
AC-14: Permitted Actions Without Identification or Authentication	B.1.12 – Permitted Actions without Identification or Authentication
AC-18: Wireless Access	B.1.17 – Wireless Access Restrictions
AC-19: Access Control for Mobile Devices	B.1.19 – Access Control for Portable and Mobile Devices B.1.18 – Insecure and Rogue Connections B.2.2 – Auditable Events B.4.5 – Device Identification and Authentication B.5.1 – Removal of Unnecessary Services and Programs C.3.3 – Malicious Code Protection C.3.4 – Monitoring Tools and Techniques C.11.3 – Baseline Configuration C.11.8 – Least Functionality

AC-20: Use of External Information Systems	B.1.22 – Use of External Systems
AC-22: Publicly Accessible Content	10 CFR 73.22(g) B.1.23 – Publicly Accessible Content
Control Family: Awareness and Training	
AT-1: Security Awareness and Training Policy and Procedures	C.10.1 – Cyber Security Awareness and Training
AT-2: Security Awareness	10 CFR 73.54(d) C.10.2 – Awareness Training
AT-3: Security Training	C.10.3 – Technical Training C.10.4 – Specialized Cyber Security Training C.10.5 – Cross-Functional Cyber Security Team C.10.6 – Situational Awareness C.10.10 – Roles and Responsibilities
AT- 4: Security Training Records	10 CFR 73.54(h) C.10.7 – Feedback C.10.8 – Security Training Records
Control Family: Audit and Accountability	
AU-1: Audit and Accountability Policy and Procedures	B.2.1 – Audit and Accountability Policy and Procedures
AU-2: Auditable Events	B.2.2 – Auditable Events
AU-3: Content of Audit Records	B.2.3 – Content of Audit Records
AU-4: Audit Storage Capacity	B.2.4 – Audit Storage Capacity
AU-5: Response to Audit Processing Failures	B.2.5 – Response to Audit Processing Failure
AU-6: Audit Review, Analysis and Reporting	B.2.6 – Audit Review, Analysis and Reporting
AU-7: Audit Reduction and Report Generation	B.2.7 – Audit Reduction and Report Generation
AU-8: Time Stamps	B.2.8 – Time Stamps
AU-9: Protection of Audit Information	B.2.9 – Protection of Audit Information
AU-10: Nonrepudiation	B.2.10 – Nonrepudiation
AU-11: Audit Record Retention	B.2.11 – Audit Record Retention
AU-12: Audit Generation	B.2.12 – Audit Generation
Control Family: Security Assessment and Authorization	
CA-1: Security Assessment and Authorization	A.3.1.1 – Security Assessment and Authorization
CA-2: Security Assessments	A.4.1 – Continuous Monitoring and Assessment A.4.1.1 – Periodic Assessment of Security Controls A.4.1.2 – Effectiveness Analysis
CA-3: Information System Connections	B.1.4 – Information Flow Enforcement C.6 – Defensive Strategy C.7 – Defense-in-Depth
CA-5: Plan of Actions and Milestones	C.13.3 – Corrective Action Program
CA-6: Security Authorization	A.3.3 – Policies and Implementing Procedures A.3.1.1– Security Assessment and Authorization A.4.2.3 – Security Reassessment and Authorization

CA-7: Continuous Monitoring	A.4.1 – Continuous Monitoring and Assessment A.4.1.1 – Periodic Assessment of Security Controls A.4.1.2 – Effective Analysis
Control Family: Configuration Management	
CM-1: Configuration Management Policy and Procedures	C.11.2 – Configuration Management Policy and Procedures
CM-2: Baseline Configuration	C.11.3 – Baseline Configuration
CM-3: Configuration Change control	10 CFR Part 50, Appendix B 10 CFR 50.54 A.4.1– Continuous Monitoring and Assessment C.11.4 – Configuration Change Control
CM-4: Security Impact Analysis	C.11.5 – Security Impact Analysis of Changes and Environment C.12.5 – Developer Security Testing
CM-5: Access Restrictions for Change	C.11.3 – Baseline Configuration C.11.6 – Access Restrictions for Change
CM-6: Configuration Settings	C.3.7 – Software and Information Integrity C.11.7 – Configuration Settings C.13.3 – Corrective Acton Program
CM-7: Least Functionality	C.11.8 – Least Functionality
CM-8: Information System Component Inventory	C.11.9 – Information System Component Inventory
CM-9: Configuration Management Plan	10 CFR Part 50, Appendix B A.3.1.3 – Identification of Critical Digital Assets A.4.2 – Change Control C.11.2 – Configuration Management Policy and Procedures
Control Family: Contingency Planning	
CP-1: Contingency Planning Policy and Procedures	C.9.1 – Contingency Planning Policy and Procedures
CP-2: Contingency Plan	10 CFR 73, Appendix C 10 CFR 73.54 10 CFR 73.55(c) 10 CFR 73.55(n) C.9.1 – Contingency Planning Policy and Procedures C.9.2 – Contingency Plan C.9.3 – Contingency Plan Testing
CP-3: Contingency Training	C.9.4 – Contingency Plan Training
CP-4: Contingency Plan Testing and Exercises	C.9.3 – Contingency Plan Testing
CP-6: Alternate Storage Site	C.9.5 – Alternate Storage Site and Location for Backups
CP-8: Telecommunication Services	10 CFR Part 50, Appendix E 10 CFR Part 73.55(j)
CP-9: Information System Backup	C.9.6 – CDA Backups
Control Family: Identification and Authentication	

IA-1: Identification and Authentication Policy and Procedures	B.4.1– Identification and Authentication Policies and Procedures
IA-2: User Identification and Authentication	B.4.2 – User Identification and Authentication
IA-3: Device Identification and Authentication	B.4.5 – Device Identification and Authentication
IA-4: Identifier Management	B.4.5 – Device Identification and Authentication B.4.6 – Identifier Management
IA-6: Authenticator Feedback	B.4.8 – Authenticator Feedback
IA-7: Cryptographic Module Authentication	B.4.9 – Cryptographic Module Authentication
Control Family: Incident Response	
IR-1: Incident Response Policy and Procedures	C.8.1– Incident Response Policy and Procedures
IR-2: Incident Response Training	C.8.2 – Incident Response Training C.8.3 – Incident Response Testing and Drills
IR-3: Incident Response Testing and Exercises	C.8.3 – Incident Response Testing and Drills
IR-4: Incident Handling	10 CFR Part 50, Appendix E 10 CFR 50.47 10 CFR 73.54 C.8.4 – Incident Handling C.8.5 – Incident Monitoring
IR-5: Incident Monitoring	C.8.5 – Incident Monitoring
IR-6: Incident Reporting	10 CFR 73.71 C.8.6 – Incident Reporting
IR-7: Incident Response Assistance	C.8.7 – Incident Response Assistance
IR-8: Incident Response Plan	10 CFR 50.47 10 CFR 50.72 10 CFR 73, Appendix C 10 CFR 73, Appendix G 10 CFR 73.55 10 CFR 73.71 10 CFR 100 C.8.8 – Cyber Incident Response Plan
Control Family: Maintenance	
MA-1: System Maintenance Policy and Procedures	C.4.1– System Maintenance Policy and Procedures
MA-3: Maintenance Tools	C.4.2 – Maintenance Tools
MA-5: Maintenance Personnel	C.4.3 – Personnel Performing Maintenance and Testing Activities
MA-6: Timely Maintenance	C.3.11– Anticipated Failure Response
Control Family: Media Protection	
MP-1: Media Protect Policy and Procedures	C.1.1 – Media Protect Policy and Procedures
MP-2: Media Access	C.1.2 – Media Access
MP-3: Media Marking	C.1.3 – Media Labeling/Marking
MP-4: Media Storage	10 CFR 73.22(g) C.1.4 – Media Storage
MP-5: Media Transport	C.1.5 – Media Transport
MP-6: Media Sanitization	C.1.6 – Media Sanitization and Disposal
Control Family: Physical and Environmental Protection	
PE-2: Physical Access Authorizations	C.5.4 – Physical Access Authorizations

PE-3: Physical Access Control	10 CFR 73.55(g) 10 CFR 73.56 C.5.3 – Physical and Environmental Protection C.5.5 – Physical Access Control
PE-4: Access Control for Transmission Medium	C.5.6 – Access Control for Transmission Medium
PE-5: Access Control for Output Devices	C.3.10 – Information Output Handling and Retention C.5.7 – Access Control for Display Medium
PE-6: Monitoring Physical Access	C.5.8 – Monitoring Physical Access
PE-7: Visitor Control	C.5.9 – Visitor Control Access Records
PE-8: Access Records	10 CFR 73.55(g) 10 CFR 73.56(o)
PE-9: Power Equipment and Power Cabling	10 CFR Part 50, Appendix A 10 CFR 50.49
PE-10: Emergency Shutoff	10 CFR Part 50, Appendix A 10 CFR Part 50, Appendix R
PE-11: Emergency Power	10 CFR 50.63
PE-12: Emergency Lighting	10 CFR Part 50, Appendix R
PE-13: Fire Protection	10 CFR Part 50, Appendix E 10 CFR Part 50, Appendix R
PE-14: Temperature and Humidity Controls	C.5.3 – Physical and Environmental Protection
PE-16 Delivery and Removal	C.11.2 – Configuration Management Policy and Procedures.
PE-18: Location of Information System Components	10 CFR Part 50, Appendix A
Control Family: Planning	
PL-1: Security Planning Policy and Procedures	10 CFR 73.54 10 CFR 73.55
PL-2: System Security Plan	10 CFR 73.54 10 CFR 73.55
PL-6: Security-Related Activity Planning	A.4.2 – Change Control
Control Family: Program Management	
PM-1: Information Security Program Plan	10 CFR 73.54(e) C.11.5 – Security Impact Analysis of Changes and Environment C.13.1 – Threat and Vulnerability Management C.13.2 – Risk Mitigation
PM-2: Senior Information Security Officer	A.3.3 – Policies and Implementing Procedures C.10.10 – Roles and Responsibilities
PM-5: Information System Inventory	C.11.9 – Component Inventory
PM-6: Information Security Measures of Performance	A.4.1.2 – Effectiveness Analysis
PM-9: Risk Management Strategy	10 CFR 73 A.3.1.2 – Cyber Security Team C.10 – Awareness and Training C.6 – Defensive Strategy
Control Family: Personnel Security	

PS-1: Personnel Security Policy and Procedures	10 CFR 26 10 CFR 73.56 C.2.1 – Personnel Security Policy and Procedures
PS-2: Position Categorization	10 CFR 73.56
PS-3: Personnel Screening	10 CFR 73.56
PS-4: Personnel Termination	C.2.2 – Personnel Termination or Transfer
PS-5: Personnel Transfer	C.2.2 – Personnel Termination or Transfer
PS-7: Third Party Personnel Security	C.5.2 – Third Party/Escorted Access
PS-8: Personnel Sanctions	10 CFR 73.56
Control Family: Risk Assessment	
RA-1: Risk Assessment Policy and Procedures	10 CFR 73.54 C.13.2 – Risk Mitigation
RA-3: Risk Assessment	10 CFR 73.1 C.13.1 – Threat and Vulnerability Management C.13.2 – Risk Mitigation C.13.3 – Corrective Action Plan
RA-5: Vulnerability Scanning	C13.1 – Threat and Vulnerability Management
Control Family: System and Service Acquisition	
SA-1: System and Services Acquisition Policy and Procedures	C.12.1 – System and Services Acquisition Policy and Procedures
SA-3: Life Cycle Support	10 CFR Part 50, Appendix B 10 CFR 73.54 C.12 – System and Services Acquisition
SA-4: Acquisitions	C.12.1 – System and Services Acquisition Policy and Procedures C.12.2 – Supply Chain Protection C.12.3 – Trustworthiness C.12.4 – Integration of Security Capabilities C.12.5 – Developer Security Testing
SA-5: Information System Documentation	C.12 – System and Services Acquisition
SA-7: User-Installed Software	10 CFR 73.54(d) C.12.6 – Licensee/Applicant Testing
SA-8: Security Engineering Principles	C.7 – Defense-in-Depth
SA-9: External Information System Services	B.1.22 – Use of External Systems C.12 – System and Services Acquisition
SA-10: Developer Configuration Management	C.12.5 – Developer Security Testing
SA-11: Developer Security Testing	C.12.5 – Developer Security Testing
SA-12: Supply Chain Protection	C.12.2 – Supply Chain Protection
SA-13: Trustworthiness	C.12.3 – Trustworthiness
Control Family: System and Communications Protection	
SC-1: System and Communications Protection Policy and Procedures	B.3.1 – Critical Digital Asset and Communications Protection Policy and Procedures
SC-2: Application Partitioning	B.3.2 – Application Partitioning and Security Function Isolation
SC-3: Security Function Isolation	B.3.2 – Application Partitioning and Security Function Isolation
SC-4: Information in Shared Resources	B.3.3 – Shared Resources
SC-5: Denial of Service Protection	B.3.4 – Denial of Service Protection

SC-7: Boundary Protection	B.1.4 – Information Flow Enforcement B.3.3 – Denial of Service Protection B.3.6 –Transmission Integrity B.3.7 – Transmission Confidentiality C.3.5 – Security Alerts and Advisories C.7 – Defense-in-depth C.11.3 – Baseline Configuration C.13.1 – Threat and Vulnerability Management C.13.2 – Risk Mitigation C.13.3 – Corrective Action Program
SC-8: Transmission Integrity	B.3.6 – Transmission Integrity
SC-9: Transmission Confidentiality	B.3.7 – Transmission Confidentiality
SC-12: Cryptographic Key Establishment and Management	B.3.9 – Cryptographic Key Establishment and Management B.4.7 – Authenticator Management
SC-13: Use of Cryptography	B.3.10 – Use of Cryptography
SC-15: Collaborative Computing Devices	B.3.11 – Unauthorized Remote Activation of Services
SC-17: Public Key Infrastructure Certificates	B.3.13 – Public Key Infrastructure Certificates
SC-18: Mobile Code	B.3.14 – Mobile Code B.5.1 – Removal of Unnecessary Services and Programs
SC-20: Secure Name/Address Resolution Service (Authoritative Source)	B.3.15 – Secure Name/Address Resolution Service (Authoritative /Trusted Source)
SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)	B.3.16 – Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22: Architecture and Provisioning for Name/Address Resolution Service	B.3.17 – Architecture and Provisioning for Name/Address Resolution Service
SC-23: Session Authenticity	B.3.18 – Session Authenticity
SC-24: Fail in Known State	B.3.22 – Fail in Known State
SC-28:Protection of Information at Rest	B.3.20 – Confidentiality of Information at Rest C.3.7– Software and Information Integrity
SC-32: Information Partitioning	C.7 – Defense-In-Depth
Control Family: System and Information Integrity	
SI-1: System and Information Integrity Policy and Procedures	C.3.1 – System and Information Integrity Policy and Procedures
SI-5: Security Alerts, Advisories, and Directives	C.3.5 – Security Alerts and Advisories
SI-6: Security Functionality Verification	C.3.6 – Security Functionality Verification
SI-7: Software and Information Integrity	C.3.7 – Software and Information Integrity
SI-9: Information Input Restrictions	C.3.8 – Information Input Restrictions
SI-10: Information Input Validation	C.3.8 – Information Input Restrictions
SI-11: Error Handling	C.3.9 – Error Handling
SI-12: Information Output Handling and Retention	C.3.10 – Information Output Handling and Retention

APPENDIX B: PARTIALLY MATCHED NIST AND NRC SECURITY CONTROLS

Appendix B describes NRC security controls that partially match NIST security controls. In some cases, the NIST security control is addressed by commitments in cyber security plan (CSP) and/or NRC regulations, rather than by one or more NRC security controls. Each NIST security control, including components and enhancements that are incorporated in the high security baseline, is listed in the left column, and the corresponding NRC security control is presented in the right column. At the bottom of each security control pair, explanations and additional insights regarding any differences in protections are provided. In many cases, NRC's robust physical and programmatic requirements offer alternate or enhanced cyber, or cyber-related, protections for CDAs at nuclear power plants. In other cases, threat vectors or vulnerabilities tolerated in typical business and governmental computing environments do not exist in the environments where CDAs reside. In all instances, the justification for NRC's implementation approach to each NIST security control item and appropriate enhancements is provided.

NIST 800-53 Rev 3 Security Control CP-10: Information System Recovery and Reconstitution	**NRC Security Control C.9.7 – Recovery and Reconstitution**
Control Family: Contingency Planning	
The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Security Control Enhancements: (2) The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*] (3) The organization provides the capability to reimage information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components 4) The organization provides the capability to reimage information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure, operation	[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.
<u>Explanation:</u> The NIST security control CP-10 is fully addressed by NRC security control C.9.7, except enhancements 2, 3, and 4 are not specifically listed in the NRC security control because of the unique nature of the nuclear power plant environment.	

For enhancement 2, CDAs at nuclear power plants are generally not transaction-based assets. The typical rollback processes used for recovery of transaction-based systems (transaction rollback or journaling) is not relevant for ICS recovery.

For enhancement 3, safety requirements that must be met prior to operating or restarting safety-related CDAs preclude immediate or automatic start-up following disruption or unscheduled CDA shutdowns. The regulations in 10 CFR 50.36(c) stipulate that, depending on the nature and severity of a disruption to safety-related equipment (CDAs), approval must be granted not only by licensee senior management, but by the NRC as well. The licensee is required to perform regression testing as a standard procedure prior to restarting CDAs that were recovered following a disruption.

For enhancement 4, safety requirements stated for the previous security control enhancement apply here as well. The licensee cannot restart CDAs that were recovered from disruption without the mandated reviews and approvals from senior management and the NRC.

NIST 800-53 Rev 3 Security Control IA-5: Authenticator Management	NRC Security Controls B.4.7– Authenticator Management B.4.3 – Password Requirements B.3.7 – Transmission Confidentiality
Control Family: Identification and Authorization	
The organization manages information system authenticators for users and devices by accomplishing the following: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator b. Establishing initial authenticator content for authenticators defined by the organization c. Ensuring that authenticators have sufficient strength of mechanism for their intended use d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators e. Changing default content of authenticators upon information system installation f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate)	**B.4.7 – Authenticator Management** [Licensee/Applicant] manages CDA authenticators by performing all of the following: • defining initial authenticator content, such as defining password length and composition, tokens, keys, and other means of authenticating • establishing administrative procedures for initial authenticator distribution; lost, compromised, or damaged authenticators; and revoking authenticators • changing default authenticators upon CDA installation • changing/refreshing authenticators [annually] **B.4.3 – Password Requirements** [Licensee/Applicant] ensures that, where used, passwords meet the following requirements: • the length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the CDA • passwords have length and complexity commensurate with the required security • passwords are changed every [describe the periods for each class of system, for example 30 days for workstations, 3 months for CDAs in the vital area, etc. 90 days] • passwords cannot be found in a dictionary and do not contain predictable sequences

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]
 	
h. Protecting authenticator content from unauthorized disclosure and modification
 	
i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators
 	
Security Control Enhancements:
(1) The information system, for password-based authentication:
(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]
 	
(b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created
 	
(c) Encrypts passwords in storage and in transmission
 	
(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization defined numbers for lifetime minimum, lifetime maximum]
 	
(e) Prohibits password reuse for [Assignment: organization-defined number] generations
 	
(2) The information system, for PKI-based authentication:
 	
(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor
	of numbers or letters
	• copies of master passwords are stored in a secure location with limited access
	• authority to change master passwords is limited to authorized personnel
	
	B.3.7 – Transmission Confidentiality
	[Licensee/Applicant] is responsible for the following:
	• configuring the CDAs to protect the confidentiality of transmitted information
	• employing cryptographic mechanisms to prevent unauthorized disclosure of information during transmission and receipt unless otherwise protected by alternative physical measures
	• implementing alternative security controls and documenting the justification for alternative security controls or countermeasures for situations in which a CDA cannot internally support transmission
	• confidentiality capabilities, including virtual private networks, or implements all of the following:
	  ○ physically restricts access to the CDA
	  ○ monitors and records physical access to the CDA to promptly detect and respond to intrusions
	  ○ uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs
	  ○ ensures that individuals who have access to the CDA are qualified
	  ○ ensures that those individuals are trustworthy and reliable in accordance with 10 CFR 73.56

(b) Enforces authorized access to the corresponding private key (c) Maps the authenticated identity to the user account (3) The organization requires that the registration process to receive [*Assignment: organization defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor) (4) The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators (5) The organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery (6) The organization protects authenticators commensurate with the classification or sensitivity of the information accessed (7) The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys (8) The organization takes [*Assignment: organization-defined measures*] to manage the risk of compromise due to individuals having accounts on multiple information systems	

Explanation:

The NIST security control IA-5 is addressed by a combination of NRC security controls. However, significant differences exist because of the need to tailor the NIST control requirements to the nuclear plant environment. NRC security controls B.4.7 (Authenticator Management) and B.4.3 (Password Requirements) address the majority of IA-5. As discussed below, specific NRC regulations target other vulnerabilities addressed by NIST security control IA-5.

Item IA-5.f includes the caveat "…if appropriate)" as part of the stipulation for this control. NRC has determined that, in consideration of how digital technologies are used within a nuclear power plant to support critical plant functions, placing minimum or maximum lifetime restrictions

and reuse conditions on authenticators is addressed by rigorous physical security mechanisms and that these serve as adequate compensatory measures.

IA-5(h)(i): The NRC security control C.1.1 requires plant personnel to "provide high assurance that the risk of unauthorized disclosure of information that could be used in a cyber attack [including authenticator content] to adversely impact the safety, security, and emergency preparedness functions of the nuclear facility is prevented." Plant personnel are committed to the performance objectives of rule 10 CFR 73.54, as well, which include providing assurances that this security control item is implemented appropriately.

Security Control Enhancements

The protections for enhancements 1(a), (b), (d) are addressed fully by NRC security control B.4.3 (Password Requirements).

The protections to encrypt passwords in storage and transmission for enhancement 1(c) is addressed by NRC security controls B.1.1 (Access Control Policy and Procedures), B.3.7 (Transmission Confidentiality), and B.4.3 (Password Requirements).

The protections to prohibit passwords reuse for enhancement 1(e) have not been selected at this time.

The protections to manage PKI-authentication for enhancements 2(a), (b), (c) were also not selected at this time due to potential difficulties in authenticating key users in emergency circumstances that posed an increased risk to safety and security in nuclear power plants.

Enhancement 3 was also not selected at this time because of the potential difficulty in arranging and securing the appropriate individuals for conducting the in-person distribution posed an increased risk to safety and security in nuclear power plants during emergency events.

NIST 800-53 Rev 3 Security Control **MA-2: Controlled Maintenance**	**NRC Security Controls** **C.4.1.– System Maintenance Policy and Procedures** **C.4.2 – Maintenance Controls** **C.4.3 – Personnel Performing Maintenance and Testing Activities**
Control Family: Maintenance	
The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site	**C.4.1.– System Maintenance Policy and Procedures** [Licensee/Applicant] developed, disseminated, and [annually] reviews the following: • responsibilities, management commitment, coordination among [Licensee/Applicant] entities, associated CDA maintenance controls, and compliance • policy and associated maintenance controls • boundaries, including the following:

maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. Security Control Enhancements: (1) The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable). (2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.	○ Owner-controlled area: the outermost protected area boundary for a plant that is outside the plant's security area. ○ Protected area: an area within the boundaries of a nuclear facility that is encompassed by physical barriers and to which access is controlled (see 10 CFR 73.2, "Definitions"). ○ Vital areas: areas containing any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Vital areas may also contain equipment or systems which would be required to function to protect public. ○ Health and safety following such failure, destruction, or release. ○ Public access area: locations outside the physical control of the plant. **C.4.2 – Maintenance Controls** [Licensee/Applicant] is responsible for the following: • approving, monitoring, and documenting the use of CDA maintenance tools • inspecting and documenting maintenance tools (e.g., diagnostic and test equipment and mobile devices, such as laptops) carried into a facility by maintenance personnel for obvious improper modifications • checking and documenting all media and mobile devices, such as laptops, containing diagnostic, CDA, and system and test programs or software for malicious code before the media or mobile device is used in or on a CDA • controlling, preventing and documenting the unauthorized removal of maintenance equipment by one of the following: ○ verifying that there is no [Licensee/Applicant] information contained on the equipment and validating the integrity of the device before reintroduction into the facility ○ sanitizing or destroying the equipment ○ retaining the equipment within the facility

	○ obtaining approval from an authority explicitly authorizing removal of the equipment from the facility • employing [automated/manual] mechanisms to restrict the use of maintenance tools to authorized personnel only and employing manual mechanisms only when CDAs or support equipment (e.g., laptops) cannot support automated mechanisms. **C.4.3 – Personnel Performing Maintenance and Testing Activities** [Licensee/Applicant] is responsible for the following: • maintaining and documenting a current list of authorized maintenance personnel consistent with its access authorization program and insider mitigation program • implementing and documenting [automated mechanism or nonautomated mechanism] to detect unauthorized use or execution of commands by an escorted individual • designating and documenting [Licensee/Applicant] personnel with required access authorization and knowledge necessary to supervise escorted personnel interacting with CDAs
Explanation: The NIST security control MA-2 is addressed through a combination of NRC security controls, except that the NRC security controls do not specify the use of automated mechanisms for scheduling and documenting maintenance activities.	
NIST 800-53 Rev 3 Security Control PE-1: Physical and Environmental Protection Policy and Procedures	**NRC Security Control C.5.1 – Physical and Environmental Protection Policy and Procedures**
Control Family: Physical and Environmental Protection	
The organization develops, disseminates, and reviews/updates: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and	**C.5.1 – Physical and Environmental Protection Policy and Procedures** For those CDAs located outside of the [Site] protected area, [Licensee/Applicant] developed, implemented, and [annually] reviews and updates the following: • a formal, documented physical and environmental protection policy that addresses the following: ○ the purpose of the physical security program as it relates to protecting the

associated physical and environmental protection controls	CDAs, ○ the scope of the physical security program as it applies to the organization's staff and third-party contractors, and ○ the roles, responsibilities, and management accountability structure of the physical security program to ensure compliance with the [Licensee/Applicant] security policy and other regulatory commitments, and • formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and operational environmental protection security controls.

Explanation:

The NIST control broadly applies a formal documented and environmental protection policy that enumerates the organization's hierarchy and duties that are associated with physical and environmental protection controls. The NRC's control C.5.1 only applies to CDAs, and only those that are located outside of the protected area boundary. The protected area boundary is a formal security boundary under the physical security program that envelops the majority of plant equipment and assets. While a formal, documented security organization including its purpose, scope, role, and responsibilities also exists within the protected area, no condition exists within those requirements to account for C.5.1 protections, or CDAs, or a combination of the two within (or beyond) the protected area boundary.

NIST 800-53 Rev 3 Security Control PE-10: Emergency Shutoff	NRC Security Control (Not Applicable)
The organization accomplishes the following: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; c. Protects emergency power shutoff capability from unauthorized activation.	N/A

Explanation:

The NIST control is partially covered through regulatory requirements under 10 CFR Part 50 Appendix A and 10 CFR Part 50 Appendix R. These regulations primarily address safety-related systems associated with reactor safety. However, no condition exists that specifically addresses

non-safety related security systems, or that each plant location where power shutoff capability exists (for all CDAs) be protected from unauthorized activation. In addition, providing safe and easy access may not be possible as many locations may involve areas of a nuclear facility where "easy access" is specifically prevented as a means to maintain safety.	
NIST 800-53 Rev 3 Security Control SI-2: Flaw Remediation	**NRC Security Control C.3.2 – Flaw Remediation**
Control Family: System and Information Integrity	
The organization accomplishes the following: a. Identifies, reports, and corrects information system flaws b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation c. Incorporates flaw remediation into the organizational configuration management process Security Control Enhancements: (1) The organization centrally manages the flaw remediation process and installs software updates automatically (2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation (3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*] (4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*]	[Licensee/Applicant] established, implemented, and documented procedures for the following purposes: • identifying the security alerts and vulnerability assessment process • communicating vulnerability information • correcting the flaw expeditiously using the configuration management process • correcting security flaws in CDAs • performing vulnerability scans and assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production Before implementing corrections, [Licensee/Applicant] documents and tests software updates related to flaw remediation to determine the effectiveness and potential side effects on CDAs. The [Licensee/Applicant] captures flaw remediation information in its Corrective Action Program.
Explanation: The NIST security control SI-2 is fully addressed by NRC security control C.3.2, except the NRC security control C.3.2 does not require the use of automated mechanisms to determine the state of information system components with regard to flaw remediation or automated patch management tools.	
NIST 800-53 Rev 3 Security Control SI-3: Malicious Code Protection	**NRC Security Control C.3.3 – Malicious Code Protection**
The organization accomplishes the following: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers,	[Licensee/Applicant] established, deployed, and documents real-time malicious code protection mechanisms at security boundary device entry and exit points, CDAs (if applicable), workstations, servers, and mobile computing

or mobile computing devices on the network to detect and eradicate malicious code: • Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means • Inserted through the exploitation of information system vulnerabilities b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures c. Configures malicious code protection mechanisms to accomplish the following: • Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy • [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Security Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms (2) The information system automatically updates malicious code protection mechanisms (including signature definitions) (3) The information system prevents non-privileged users from circumventing malicious code protection capabilities	devices (i.e., calibrators) on the network to detect and eradicate malicious code resulting from the following: • data communication between systems, CDAs, removable media, or other common means • exploitation of CDA vulnerabilities [Licensee/Applicant] documents and updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with the [Licensee/Applicant]'s configuration management policy and procedures. [Licensee/Applicant] documents and configures malicious code protection mechanisms to ensure the following: • Scans are performed of security boundary devices, CDAs (if applicable), workstations servers, and mobile computing devices weekly and real-time scans of files from external sources are performed as the files are downloaded, opened, or executed • Infected files are disinfected and quarantined • [Licensee/Applicant] documents and employs malicious code protection software products from multiple vendors as part of a defense-in-depth strategy and addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the CDA [Licensee/Applicant] centrally manages malicious code protection mechanisms to achieve the following: • The CDAs prevent users from circumventing malicious code protection capabilities • the CDAs update malicious code protection mechanisms only when directed by a privileged user [Licensee/Applicant] does not allow users to introduce unauthorized removable media into the CDAs. [Licensee/Applicant] disables all media interfaces (e.g., USB ports) that are not required for the operation of the CDA.

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

Explanation:

The NRC security control C.3.3 addresses each NIST SI-3 security control item and required security control enhancements, with the exception of enhancement 2 (automated update of malicious code protection mechanisms).

As per tailoring guidance stipulated by NIST SP 800-53, Appendix I, regarding compensating measures, if ICSs do not support the automated update of malicious code protection mechanisms, NRC requires plant personnel to update malicious code protection mechanisms only when directed by a privileged user who conducts an assessment of the proposed updates before executing the protection actions.

NIST 800-53 Rev 3 Security Control SI-4: Information System Monitoring	NRC Security Control C.3.4 – Monitoring Tools and Techniques

The organization accomplishes the following:
a. Monitors events on the information system in accordance with [*Assignment: organization defined monitoring objectives*] and detects information system attacks
 	
b. Identifies unauthorized use of the information system
 	
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization
 	
d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information
 	
e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable Federal laws, Executive Orders, directives, policies, or regulations
	[Licensee/Applicant] is responsible for the following:
	• monitoring events on the CDAs
	• detecting CDAs attacks
	• detecting and blocking unauthorized connections
	• retaining event logs in accordance with information retention requirements
	• identifying unauthorized use of the CDAs
	• monitoring devices that are deployed to provide visibility across CDAs for the following capabilities:
	  ○ to collect information to detect attacks, unauthorized behavior and access, and authorized access
	  ○ to track specific types of transactions of interest to [Licensee/Applicant]
	
	[Licensee/Applicant] heightens the level of monitoring activity whenever [Licensee/Applicant] or the U.S. Nuclear Regulatory Commission (NRC) determines that there is an indication of increased risk to the safety, security, or emergency operations of the site.
	
	[Licensee/Applicant] documents, interconnects, and configures individual intrusion detection tools into a plantwide intrusion detection system using common protocols.

Security Control Enhancements: (1) The organization employs automated tools to support near real-time analysis of events (2) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions (3) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*] (4) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities	[Licensee/Applicant] tests cyber intrusion detection and prevention systems consistent with the timeframe defined in Nuclear Energy Institute (NEI) 03-12, Section 20.1, for intrusion detection systems, and before being placed back in service after each repair or inoperative state. [Licensee/Applicant] documents and employs automated tools to support near real-time analysis of events. [Licensee/Applicant] documents and employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. [Licensee/Applicant] monitors, logs, and documents inbound and outbound communications for unusual or unauthorized activities or conditions. Monitoring capabilities provide real-time alerts when indications of compromise or potential compromise occur. [Licensee/Applicant] prevents users from circumventing intrusion detection and prevention capabilities. [Licensee/Applicant] notifies and documents incident response personnel of suspicious events and takes the least-disruptive actions to SSEP functions to investigate and terminate suspicious events. [Licensee/Applicant] documents and protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion. [Licensee/Applicant] uses competent cyber security personnel to randomly test and document intrusion monitoring tools. [Licensee/Applicant] documents and makes provisions to ensure that encrypted traffic is visible to monitoring tools. [Licensee/Applicant] analyzes and documents outbound communications traffic at the external boundary of CDAs (i.e., system perimeter) and, at selected interior points within the CDAs infrastructure to discover anomalies.

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

Explanation:

The NIST security control SI-4 is fully addressed by the NRC security control B.3.4 except for item SI-4(e). The NRC determined that NIST security control item SI-4(e) is not applicable to licensed nuclear power plants, because the NRC has no regulatory basis to require facility personnel to obtain legal opinion with regard to information system monitoring activities to meet Federal laws, Executive Orders, directives, policies, or regulations.

Moreover, the NRC control offers additional protections than those specified by NIST security control SI-4 to address use on industrial control systems. For example, the NRC security control also requires the determination of whether candidate monitoring tools and techniques (including automated mechanisms) may adversely impact the performance of CDAs, in which case alternative countermeasures would be implemented that provide equivalent protective measures.

APPENDIX C: NON-MATCHING NIST AND NRC SECURITY CONTROLS

NIST security control implementation policy (especially security controls within the high baseline) stipulates organizations should either incorporate all protections into their information security programs or other means that fully address the vulnerability specified by NIST. This appendix presents those NIST security controls that do not have corresponding NRC security controls and were not explicitly incorporated into the suite of NRC security controls.

NIST 800-53 Rev 3 Security Control	Explanation
Control Family: Access Control	
AC-10: Concurrent Session Control	The NRC determined that allowing concurrent system account sessions to be launched by a single user or account presented an unacceptable risk to critical SSEP functions. Allowing multiple user sessions opens the possibility for profiles and passwords to be shared. In addition, unauthorized persons could access sessions that are inadvertently left open. Therefore, the NIST security control AC-10 was not included in the suite of NRC security controls.
AC-17: Remote Access	The NRC determined that allowing remote access to critical systems and CDAs presented an unacceptable risk to critical SSEP functions. Therefore, remote access to CDAs is prohibited in the highest security levels. Furthermore, the comprehensive defensive-in-depth strategy that emphasizes isolation and compartmentalization of CDAs would be compromised with the introduction of remote user access.
Control Family: Contingency Planning	
CP-7: Alternate Processing Site	The NRC does not require an alternative processing facility that is geographically removed from the nuclear power plant. Nuclear power plants do have technical support centers located in close proximity to the control room with limited displays and data available for senior plant management and technical personnel to support control room operations personnel during emergency situations. Given that the primary goal of the NRC is to protect public health and safety by ensuring and maintaining the safe shutdown of the nuclear reactor in the event of an emergency and maintenance of the reactor in a safe mode, a backup shutdown control panel is also available outside the control room in the event that a manual shutdown is required (if the control room is not habitable).

Control Family: Identification and Authentication	
IA-8: Identification and Authentication (Non-organization Users)	This security control was not included in the RG 5.71 because users requiring access to CDAs at operating nuclear power plants include employees and non-employees that are deemed to have equivalent status as organizational employees. Non-employees, such as contractors and vendor staff, are subject to the identical security clearance procedures as plant employees (background check, finger printing, drug tests, access authorizations). Therefore, the IA-8 security control does not apply.
Control Family: Maintenance	
MA-4: Non Local Maintenance	The NRC does not offer a corresponding security control to NIST security control MA-4. The NRC security control C.6 discusses the requirements for defensive strategy. This strategy emphasizes isolation and compartmentalization of CDAs that are associated with SSEP functionality and discourages the use of CDA maintenance executed via remote network access.
Control Family: Physical and Environmental Protection	
PE-17: Alternate Work Site	The NIST security control PE-17 was not selected for the suite of NRC security controls because nuclear power plants do not have alternate work sites with backup CDAs associated with SSEP functions covered by the NRC cyber security program.
Control Family: Planning	
PL-4: Rules of Behavior	In consideration of security awareness, technical, and specialized cyber security training security controls, and those governing the retention of training records for individuals having access to CDAs, NIST security control PL-4 was not selected for inclusion in the suite of NRC security controls at this time.
PL-5: Privacy Impact Assessment	NIST security control PL-5 was not selected for inclusion in the NRC suite of security controls because of regulatory constraints. Commercial entities (e.g., nuclear power plants) are not required to adhere to OMB policy.
Control Family: Personnel Security	
PS-6: Access Agreements	The NIST security control PS-6 was not selected for inclusion in the NRC suite of security controls because of regulatory constraints. The requirement for signed access agreements on the part of individuals is outside of the NRC's regulatory authority.
Control Family: Risk Assessment	

RA-2: Security Categorization	All systems covered under the NRC's cyber security regulations (i.e., 10 CFR 73.54), have been designated by the NRC as high impact. Therefore, licensees do not have to perform this process.
Control Family: System and Services Acquisition	
SA-2: Allocation of Resources	The NIST security control SA-2 was not selected for inclusion in the NRC suite of security controls because of regulatory constraints. The requirement for allocating nuclear power plant resources and capital planning is outside the NRC's regulatory authority.
SA-6: Software Usage Restrictions	The NIST security control was not selected for inclusion in the NRC suite of security controls because of regulatory constraints. The intent of the NIST security control is the management and monitoring of software copyright infringement that could occur because of inappropriate and unauthorized reproduction, sharing, distribution, et cetera. While the listed practices can introduce vulnerabilities into the CDA environment, the requirement for managing software usage, as described by NIST, is outside of the NRC's regulatory authority.
Control Family: System and Communications Protection	
SC-10: Network Disconnect	The NIST security control SC-10 was not included in the suite of NRC security controls because of the potential to impact safety. At nuclear power plants, network communication sessions are generally left open for long periods of time to facilitate monitoring of critical safety control systems. In such cases, the implementation of this security control would have a direct impact on the operational integrity of safety functions at the nuclear power plant.
SC-14: Public Access Protections	The NIST security control SC-14 was not included in the suite of NRC security controls because CDAs and the data processed, stored, and transmitted by CDAs, performing or supporting safety, security, or emergency preparedness functions are not publicly available. The following NRC non-corresponding security controls discuss CDAs not being exposed to or impacted by access to publicly available information systems. NRC security control B.3.6 requires configuring CDAs to protect the integrity of transmitted information. NRC security control B.3.7 requires configuration of the CDAs to protect

	the confidentiality of transmitted information. NRC security control B.3.8 requires the configuration of CDAs to use trusted communication paths between the user and the security functions of the CDAs, which includes authentication and reauthentication at a minimum.
SC-19: Voice Over Internet Protocol	This security control was not included in the suite of NRC security controls because the use of VoIP would be governed by the same criteria as other technologies in terms of security review and authorization. NRC security controls such as B.3.5 Resource Priority, B.3.6 Transmission Integrity, B.3.7 Transmission Confidentiality, and B.3.8 Trusted Path, among others, would be employed to ensure VOIP technology is implemented in a manner that meets the requirements of regulation 10 CFR 73.54.
Control Family: System and Information Integrity	
SI-8: Spam Protection	This security control applies less to the industrial control systems' environments than to corporate systems, putting these requirements outside the scope of NRC's regulatory authority for cyber security at the nuclear power plants. As per the tailoring guidance for security control SI-8 provided by NIST SP 800-53, Appendix I, ICSs do not generally employ spam protection because CDAs do not use electronic mail or web access services and functions. Also, the defense-in-depth protective strategy specified in NRC security control C.7 prohibits these types of services and functions from existing on CDAs or from connecting to the protected environment. Therefore this security control is not part of the NRC security control baseline.
Control Family: Program Management	
PM-3: Information Security Resources	The NIST security control PM-3 was not selected for inclusion in the NRC suite of security controls because of regulatory constraints. The requirement to complete resource planning and investment forms that are part of Federal agency capital planning procedures is outside of the NRC's regulatory authority.
PM-4: Plan of Action and Milestones Process	The NRC does not offer a corresponding security control to NIST security control PM-4. The vulnerability covered by the NIST security control PM-4 is addressed through a combination of regulatory requirements and an NRC non-corresponding security control.

	Specifically, 10 CFR 73.54 (e)(2)(iii) requires corrective actions to address vulnerabilities and therefore to ensure that security controls are in place and working effectively. The requirement to maintain corrective actions in plans of action and milestones is a Federal IT security mandate and is not applicable to nuclear power plants. In addition, the NRC security control C.13.3 requires the use of a Corrective Action Program which provides a process to document and track remediation of cyber security issues.
PM-7: Enterprise Architecture	The NIST security control PM-7 was not selected for the suite of NRC security controls because of regulatory constraints. The NRC does not have regulatory authority to require nuclear power plants to develop, implement, and manage sitewide system architectures that align with the Federal Enterprise Architecture (FEA).
PM-8: Critical Infrastructure	The NIST security control PM-8 was not selected for the suite of NRC security controls because it addresses a Federal activity that does not apply to nuclear power plants.
PM-10: Security Authorization Process	The NRC does not offer a corresponding security control to NIST security control PM-10. The vulnerability covered by the NIST security control PM-10 is addressed by a CSP commitment. CSP commitment A.3.1.2 requires the formation of a cyber security team by defining and documenting roles, responsibilities, authorities, and functional relationships, and ensuring that these are understood by site organizations and individuals (including employees, subcontractors, temporary employees, visiting researchers, and vendor representatives) at every level in the organization. The cyber security team implements the cyber security program that includes executive or officer-level accountability in addition to program management oversight responsibilities. This equates to roles typically referred to in Federal government as designated approving authorities and system owners.
PM-11: Mission/Business Process Definition	The NIST security control PM-11 was not selected for the suite of NRC security controls because the actions required in this security control were performed by the NRC as part of developing its cyber security regulations. The NRC determined that cyber security requirements should apply to safety,

	important-to-safety, security, and emergency preparedness functions. The NRC does not have authority to impose requirements on the entire mission/business processes of nuclear power plants for activities that fall outside the scope of NRC's regulatory jurisdiction.

APPENDIX D: SECURITY CONTROLS UNIQUE TO NRC

This appendix discusses NRC security controls developed for use within the nuclear sector and for which there is no corresponding security control in the NIST baseline. When formulating these controls, the NRC considered security controls discontinued by NIST in Revision 3 of NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations." The NRC decided to incorporate some of the discontinued NIST security controls, where appropriate, to ensure cyber security programs at power reactor sites achieve the performance requirement of NRC's security regulations. As a result, in some cases an NRC security control may be a match with a NIST security control that is no longer included (i.e., discontinued) in the NIST high baseline.

NRC Security Control	Explanation
B.1.9 – Previous Logon Notification	This security control is related to the NIST security control AC-9, Previous Logon (Access) Notification, which was withdrawn by NIST. NRC security control B.1.9 addresses the potential threat caused by a failure to detect misuse of credentials by an individual other than an assigned and authorized user. Implementation of this security control provides users with information that could determine if their accounts are being accessed by unauthorized individuals or if access attempts are being made by unauthorized parties.
B.1.11 – Supervision and Review – Access Control	This security control is related to the NIST security control AC-13, Supervision and Review – Access Control, which was withdrawn by NIST. NRC security control B.1.11 addresses the potential threat caused by a failure to detect unauthorized access or misuse of user credentials because of a lack of supervision and review of user activities. Implementation of this security control provides organizations with additional assurance that management reviews of cyber activity (in this case user access and other activity) are occurring on an ongoing basis in an effort to address the threat of unauthorized access to CDAs.
B.1.13 – Automated Marking	This security control is related to the NIST security control AC-15, Automated Marking, which was withdrawn by NIST. NRC security control B.1.13 addresses the potential threat caused by spillage, leaking, or mishandling of protected data due to improper marking of CDA output or lack of clear handling instructions. Implementation of this security

NRC Security Control	Explanation
	control allows organizations to accomplish the following: identify various levels or categories of data sensitivity and associated handling instructions, establish a standard naming convention for these categories, and ensure that any hard or soft copy output generated by CDAs/CSs are automatically marked using this standard convention.
B.1.14 – Automated Labeling	This NRC security control addresses the potential threat caused by spillage, leaking, or mishandling of protected data due to improper marking of CDA data. Unlike “marking,” which refers to human-readable security attributes, “labeling” denotes digital or computer-readable attributes. As CDA data is moved across networks or portable electronic devices, implementation of this security control provides assurance that the information retains an indication of its security classification so that system and application software can process and protect it appropriately.
B.1.15 – Network Access Control	This NRC security control addresses the potential threat caused by unauthorized access to CDAs, CDA networks, or CDA data through failure to restrict connectivity to authorized and approved devices. While remote access (NIST security control AC-17) is not applicable because it is prohibited as a path to CDAs, this security control emphasizes the need to protect critical assets from unauthorized connectivity. Implementation of this security control provides assurance that no devices are able to connect to CDAs or associated networks without prior express authorization.
B.1.16 – Open/Insecure Protocol Restrictions	This NRC security control addresses the potential threat to CDAs caused by failure to restrict or eliminate known insecure protocols. Implementation of this security control provides assurance that communications protocols, which lack security features, are sufficiently restricted to minimize risks to CDAs that use them.
B.1.18 – Insecure and Rogue Connections	This NRC security control addresses the potential threat to CDAs caused by a failure to properly monitor or manage communications connections. Implementation of this security control provides assurance that all

NRC Security Control	Explanation
	connections and communication devices on CDA networks and critical systems are known, identified, authorized, properly configured, and operating in accordance with policy, procedure, and the site's defensive architecture.
B.1.20 – Proprietary Protocol Visibility	This NRC security control addresses the potential threat to CDAs caused by the inability to assess, monitor, or secure a communications channel due to a lack of visibility into the technical aspects of the protocol used. Implementation of this security control provides assurance that proprietary or closed protocols do not operate in the CDA environment where their presence can compromise security and provide opportunities for cyber-based attacks.
B.1.21 – Third Party Products and Controls	This NRC security control addresses circumstances where IT security solutions from third-party suppliers may not be installed on CDAs because of licensing arrangements and service agreements with commercial vendors. If service agreements or licensing arrangements prohibit the upgrading of security capabilities of the acquired products, the employment of alternative security controls must be accomplished to mitigate the vulnerabilities created by the inability to deploy the third-party products.
B.3.5 – Resource Priority	This NRC security control addresses the threat caused by loss of availability of CDA functionality because of resource exhaustion of lower-priority CDA functions or processes. In a typical digital networking environment, CDAs may share resources such as bandwidth, access control devices, routing devices, mass storage units, et cetera. The NRC security control ensures that the sharing of digital resources does not allow processes associated with lower functional priorities to interfere with or deny resources or access to resources required by CDAs with a higher processing priority.
B.3.8 – Trusted Path	This NRC security control addresses the threat caused by inadvertent or malicious exposure or capture of valid user credentials during an authentication/user login process. It also addresses the threat to CDA functional integrity and availability because of a failure to protect transmitted data. The security control

NRC Security Control	Explanation
	ensures that applicable communication paths are implemented that verify user and CDA credentials, encrypt information flow where feasible, and enforce the execution of security measures throughout the duration of data transmission sessions.
B.3.12 – Transmission of Security Parameters	This NRC security control is related to the NIST security control SC-16, Transmission of Security Attributes, which was withdrawn by NIST. Security control B.3.12 addresses the potential threat to CDAs caused by spillage of sensitive data because of failure to preserve parameters during transfer or transmission. Implementation of this security control provides assurance that sensitive data will not be disclosed to unauthorized parties because of failure to maintain the binding between the data and its assigned security parameters.
B.3.19 – Thin Nodes	This NRC security control is related to the NIST security control SC-25, Thin Nodes, which was withdrawn by NIST. Security control B.3.19 addresses the potential threat to CDAs caused by the presence of data, application software, and sensitive information on client CDAs. The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint and may reduce the exposure of CDAs to a successful attack.
B.3.21 – Heterogeneity/Diversity	This NRC security control is related to the NIST security control SC-29, Heterogeneity, which was withdrawn by NIST. Security control B.3.21 addresses the potential threat to CDAs of a heightened impact of compromise because of a large percentage of systems sharing a common flaw or weakness. The deployment of a diverse or heterogeneous assortment of hardware and software platforms reduces the risk of a successful exploitation compromising significant portions of a network environment because of a common flaw or vulnerability.
B.4.4 – Nonauthenticated Human Machine Interaction Security	This NRC security control addresses the threat that exists when CDAs, because of technical or operational limitations, cannot support authentication methods. In circumstances in which CDAs do not permit individual authentication for accessing critical processes, alternative safeguards must be provided to

NRC Security Control	Explanation
	ensure that access and use of CDAs is limited to authorized personnel, and that actions performed on CDAs can be attributed to specific individuals.
B.5.2 – Host Intrusion Detection System	This NRC security control addresses the threat to CDAs from the failure to detect, prevent, and mitigate attacks due to insufficient system-level protection measures. The security control requires that intrusion detection software be installed on critical systems to monitor system or network traffic for malicious or unauthorized activities occurring on discrete hosts (or CDAs).
B.5.3 – Changes to File System and Operating System Permissions	This NRC security control addresses the threat to CDAs from compromise or attack due to insufficiently restrictive permissions on files, systems, and functions. The security control ensures that user permissions and access to critical files and functions are configured at the lowest privilege level possible. In cases where attackers successfully acquire user access, implementing least privilege access and capability helps mitigate the impact of malicious activity.
B.5.4 – Hardware Configuration	This NRC security control addresses the threat to CDAs from improperly secured system hardware. The security control ensures that, by reducing or disabling access to unnecessary or unused communications interfaces, limiting access to those interfaces, or reducing the privilege levels to a minimum, and documenting both the hardware configurations and procedures for modifying those configurations, system hardware is protected from compromise due to a malicious attack.
B.5.5 – Installing Operating Systems, Applications, and Third-Party Software Updates	The NRC security control addresses the threat to CDAs due to insufficient management of software updates to CSs and CDAs. The security control requires that security patches received from vendors and other third party entities are applied, tested, and controlled in a standardized manner.
C.3.11 – Anticipated Failure Response	This NRC security control is related to the NIST security control SI-13, Predictable Failure Prevention, which was withdrawn by NIST. Security control C.3.11 addresses the threat posed to critical plant functions caused by the failure of CDAs because of unanticipated loss of CS components.

NRC Security Control	Explanation
	The security control stresses compliance with existing requirements that protect the availability of CDAs (e.g., technical specifications, preventative maintenance, security plans, emergency plans, correction action programs), and includes additional measures to take if these requirements do not apply to a specific CDA.
C.10.9 – Contacts with Security Groups and Associations	This NRC security control is related to the NIST security control AT-5, Contacts with Security Groups and Associations, which was withdrawn by NIST. This security control addresses lack of access to current and prompt information on cyber threats, trends, and evolving technologies. Implementation of this security control provides assurance that the licensee is informed of current developments in cyber security, trends, and technologies.
C.12.6 – Licensee/Applicant Testing	This NRC security control addresses the compromise of the security of CDAs due to the introduction of insecure or insufficiently tested application or system software. This is an added measure beyond developer security testing (NRC security control C.12.5 and NIST security control SA-11), where a licensed utility validates security tests conducted by developers and ensures software security requirements are adequately addressed.
C.13.2 – Risk Mitigation	This NRC security control addresses the failure of cyber security protections because of ineffective implementation of the strategies, security controls, processes, and procedures specified by other NRC security controls and related commitments in the licensed utilities' NRC-approved Cyber Security Plans. Implementation of this security control ensures that effective measures are employed to protect CDAs from current and future threats, as specified in the security control descriptions, and are performing continuous monitoring to mitigate known and potential risks.

APPENDIX E: COMPARISON BETWEEN RG 5.71 SECURITY CONTROLS AND NERC CIP (UPDATED MARCH, 2012) STANDARDS

This section compares the cyber security requirements provided by the North American Energy Reliability Corporation (NERC) for the bulk electric producers under the title Critical Infrastructure Protections (CIP) and the security controls provided by the NRC in Regulatory Guide 5.71, Revision 0 for new and operating nuclear power reactor facilities. The table is sequenced according to the NERC CIP requirements. For each NERC CIP requirement, a corresponding NRC security control, or group of controls, is provided. Additional information is provided in those cases where a NRC security control does not provide equivalency to a NERC CIP requirement, or other NRC regulations apply.

NERC CIP Requirements	Matching NRC Controls	Additional Information
CIP-002-4 R1 Critical Asset Identification	C.11.9 – Component Inventory A.3.1.3 – Identification of Critical Digital Assets	N/A
CIP-002-4 R2 Critical Cyber Asset Identification	C.11.9 – Component Inventory	N/A
CIP-002-4 R3 Critical Cyber Asset Annual Approval	C.11.9 – Component Inventory	CSP commitment A.4.2.1 provides additional programmatic guidance for managing inventories of CDAs.
CIP-003-4 R1 Cyber Security Policy	B.1.1 – Access Control Policy and Procedures B.3.1 – Critical Digital Asset and Communications Protection Policy and Procedures B.4.1 – Identification and Authentication Policies and Procedures C.1.1 – Media Protection Policy and Procedures C.2.1 – Personnel Security Policy and Procedures C.3.1 – System and Information Integrity Policy and Procedures, C.4.1 – System Maintenance Policy and Procedures	N/A

	C.5.1 – Physical and Environmental Protection Policies and Procedures C.8.1 – Incident Response Policy and Procedures C.9.1 – Contingency Planning Policy and Procedures C.10 – Awareness and Training C.11.2 – Configuration Management Policy and Procedures	
CIP-003-4 R2 Leadership	A.3.3 – Policies and Implementing Procedures	N/A
CIP-003-4 R3 Exceptions	N/A	The NRC guidance does not include provisions for policy exceptions.[4]
CIP-003-4 R4 Information Protection	Appendix A, Regulatory Guide 5.71	Licensed nuclear facilities' cyber security programs are established in accordance with their NRC-approved cyber security plans (CSPs). A CSP template is provided in Appendix A of Regulatory Guide 5.71.
CIP-003-4 R5 Access Control	B.1 – Access Controls	N/A
CIP-003-4 R6 Change Control and Configuration Management	C.11 – Configuration Management	N/A
CIP-004-4 R1 Security Awareness	C.10.1 – Cyber Security Awareness and Training C.10.2 – Awareness Training C.10.3 –Technical Training	The NRC security controls address all aspects of the NERC requirements, with one exception. The NRC security controls do not specify a periodicity for when security awareness training is to be conducted. However, the NRC security control C.10.3, Technical Training, requires that specialized training for individuals with cyber security responsibilities occur annually.

[4] As of February 15, 2013 the NERC Board of Trustees approved the retirement of the CIP-003-4 R3 requirement, and is now pending regulatory approval.

CIP-004-4 R2 Training	C.10.1 – Cyber Security Awareness and Training C.10.3 – Technical Training C.10.4 – Specialized Cyber Security Training C.10.6 – Situational Awareness C.10.8 – Security Training Records	N/A
CIP-004-4 R3 Personnel Risk Assessment	C.2.1 – Personnel Security Policy and Procedures	The NRC security control, in conjunction with the regulation mandating licensee implementation of stringent personnel security policies (10 CFR 73.56), addresses all aspects of the NERC requirement.
CIP-004-4 R4 Access	B.1.1 – Access Control Policy and Procedures C.2.2 – Personnel Termination or Transfer	N/A
CIP-005-4a R1 Electronic Security Perimeter	A.3.1.3 – Identification of Critical Digital Assets A.3.1.4 – Reviews and Validation Testing A.3.1.5 – Defense-in-Depth Protective Strategies	N/A
CIP-005-4a R2 Electronic Access Controls	B.1.1 – Access Control Policy and Procedures B.1.2 – Account Management B.1.8 – System Use Notification B.1.17 – Wireless Access Restrictions B.1.19 – Access Control for Portable and Mobile Devices B.3.1 – Critical Digital Asset and Communications Protection Policy and Procedures B.4.2 – User Identification and	N/A

	Authentication C.11.8 – Least Functionality	
CIP-005-4a R3 Monitoring Electronic Access	B.2 – Audit and Accountability controls	N/A
CIP-005-4a R4 Cyber Vulnerability Assessment	C.13 – Security Assessment and Risk Management controls	N/A
CIP-005-4a R5 Documentation Review and Maintenance	A.5 – Document Control and Records Retention and Handling B.2.6 – Audit Review, Analysis and Reporting C.11.3 – Baseline Configuration C.11.4 – Configuration Change Control	N/A
CIP-006-4d R1 Physical Security Plan	C.5.1 – Physical and Environmental Protection Policies and Procedures C.5.4 – Physical Access Authorizations C.5.9 – Visitor Control Access Records	In addition, the NRC regulation 10 CFR 73.55(c)(3) requires licensees to develop and maintain a physical security plan and the regulation 10 CFR 73.56(a) requires licensees to establish and maintain a personnel access authorization program.
CIP-006-4d R2 Protection of Physical Access Control Systems	A.3.1.6 – Application of Security Controls A.3.2 – Incorporating the Cyber Security Program into the Physical Protection Program A.4.2.2 – Security Impact Analysis of Changes and Environment B.1.10 – Session Lock B.3.2 – Application Partitioning and Security Function Isolation B.3.6 – Transmission Integrity B.3.7 – Transmission Confidentiality B.4.2 – User Identification and Authentication	The NRC regulation 73.55(e) also provides assurance that licensees meet the intent of this NERC security requirement.

	B.4.4 – Nonauthenticated Human Machine Interaction Security B.4.5 – Device Identification and Authentication C.3.6 – Security Functionality Verification C.5 – Physical and Environmental Protection C.6 – Defensive Strategy	
CIP-006-4d R3 Protection of Electronic Access Control Systems	C.7 – Defense-in-Depth	N/A
CIP-006-4d R4 Physical Access Controls	C.5.5 – Physical Access Control C.6 – Defensive Strategy A.3.2 – Incorporating the Cyber Security Program into the Physical Protection Program	N/A
CIP-006-4d R5 Monitoring Physical Access	C.5.5 – Physical Access Control C.5.8 – Monitoring Physical Access	Additionally, practices implemented to meet the NRC physical security regulations specified in 73.55(i) also address this NERC stipulation.
CIP-006-4d R6 Logging Physical Access	C.5.8 – Monitoring Physical Access	Additionally, practices implemented to meet the NRC physical security regulations specified in 73.55(i) also address this NERC stipulation.
CIP-006-4d R7 Access Log Retention	C.5.9 – Visitor Control Access Records A.5 – Document Control and Records Retention and Handling	N/A
CIP-006-4d R8 Maintenance and Testing of Physical Control Systems	A.4.1.2 – Effectiveness Analysis[5] A.5 – Document Control and Records Retention Handling	The NRC physical security regulation requires licensees to maintain and rigorously and periodically test physical control systems. 10 CFR 73.55(m) requires licensees to review (including testing) all aspects of the physical security program (including cyber security programs) at least biannually. 10

[5] The regulatory guidance states that control effectiveness is to be reviewed on an annual basis

		CFR 73.55(n) requires licensees to implement, test, and maintenance activities on an ongoing basis to ensure the effectiveness of the physical security programs. Compliance with these rules allows licensees to meet the requirements of the NERC security control.
CIP-007-4 R1 Test Procedures	C.11 – Configuration Management	N/A
CIP-007-4 R2 Ports and Services	C.11.8 – Least Functionality C.13.2 – Risk Mitigation	N/A
CIP-007-4 R3 Security Patch Management	C.3.2 – Flaw Remediation B.5.5 – Installing Operating Systems, Applications and Third-Party Software Updates C.13.2 – Risk Mitigation	N/A
CIP-007-4 R4 Malicious Software Prevention	C.3.3 – Malicious Code Protection C.3.4 – Monitoring Tools and Techniques C.13.2 – Risk Mitigation	N/A
CIP-007-4 R5 Account Management	B.1 – Access Controls B.2 – Audit and Accountability	N/A
CIP-007-4 R6 Security Status Monitoring	B.2 – Audit and Accountability C.3.4 – Monitoring Tools and Techniques	N/A
CIP-007-4 R7 Disposal and Redeployment	C.1.1 – Media Protection Policy and Procedures C.1.6 – Media Sanitation and Disposal	N/A
CIP-007-4 R8 Cyber Vulnerability Assessment	C.13.1 – Threat and Vulnerability Management	N/A
CIP-007-4 R9 Documentation Review and Maintenance	C.11.3 – Baseline Configuration C.11.4 – Configuration Change Control	N/A
CIP-008-4 R1 Cyber Security Incident Response Plan	C.8.1 – Incident Response	N/A

CIP-008-4 R2- Cyber Security Incident Documentation	B.2.11 – Audit Record Retention A.5 – Document Control and Records Retention and Handling	N/A
CIP-009-4 R1 Recovery Plans	C.9.2 – Contingency Plan	N/A
CIP-009-4 R2 Exercises	C.9.3 – Contingency Plan Testing	N/A
CIP-009-4 R3 Change Control	C.8.1 – Incident Response Policy and Procedures	N/A
CIP-009-4 R4 Backup and Restore	C.9.6 – CDA Backups	N/A
CIP-009-4 R5 Testing Backup Media	C.9.7 – Recovery and Reconstitution	N/A

APPENDIX F: LOCATION OF REFERENCED DOCUMENTS

Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” Revision 0	ML090340159
NIST Special Publication 800-37 Revision 1: “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”	ML14218A804
NIST Special Publication 800-53 Revision 3: “Recommended Security Controls for Federal Information Systems and Organizations”	ML14218A808
NUREG/CR-6847, “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants”	ML043200191
Nuclear Energy Institute (NEI) 04-04, “Cyber Security Program for Power Reactors”	ML072420411
NRC RG 1.152, Revision 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”	ML053070150
Branch Technical Position 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”	ML070670183
Nuclear Energy Institute (NEI) 08-09, “Cyber Security Plan for Nuclear Power Reactors”	ML101180437
Nuclear Energy Institute (NEI) 13-10, “Cyber Security Control Assessments”	ML13338A622
North American Energy Reliability Corporation (NERC) Critical Infrastructure Protections (CIP)	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-7141

2. TITLE AND SUBTITLE
The U.S. NRC Cyber Security Regulatory Framework for Nuclear Power Reactors

3. DATE REPORT PUBLISHED

MONTH	YEAR
November	2014

4. FIN OR GRANT NUMBER

5. AUTHOR(S)
C. Chenoweth (MAR)
J. Green (MAR)
T. Shaw (MAR)
M. Shinn (MAR)
G. Simonds (MAR)

6. TYPE OF REPORT
Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)
MAR, Incorporated
1803 Research Boulevard, Suite #204
Rockville, MD 20850-6106

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)
Cyber Security Directorate
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)
The NUREG/CR-7141, "the U.S. NRC Cyber Security Regulatory Framework for Nuclear Power Reactors" provides an overview of NRC regulatory framework for cyber security, comparing programmatic guidance contained within Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," Revision 0, to both the National Institute of Standards and Technology (NIST) Risk Management Framework found in NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," Revision 1, as well as to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Further, this framework correlates the high baseline security controls published by NIST in Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3, to those contained in Appendices B and C of RG 5.71 ("Technical Security Controls" and "Operational and Management Security Controls", respectively). This report is not regulatory guidance and does not supersede policy decisions made by the NRC on behalf of security programs defined in the NRC's regulations, or rules. Nor does this report impose any new requirements or interpretations of NRC regulations that could be used for complying with a license's approved cyber security plan, as defined in Title 10 of the Code of Federal Regulations (CFR) Part 73.54, "Protection of Digital Computer and Communication Systems and Networks" (10 CFR 73.54).

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Cyber Security
Framework
NIST Special Publication 800-37
North American Electric Reliability Corporation (NERC)
Critical Infrastructure Protection (CIP) standards
Regulatory Guidance (RG) 5.71

13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Printed
on recycled
paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG/CR-7141

The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors

November 2014