U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

13.6.6 CYBER SECURITY PLAN

REVIEW RESPONSIBILITIES

Primary - Office of Nuclear Security and Incident Response

Secondary - None

I. AREAS OF REVIEW

The U.S. Nuclear Regulatory Commission (NRC) evaluates the applicant/licensee's plan to provide high assurance that the digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions, as well as support systems and equipment, which if compromised, would adversely impact safety, security, or emergency preparedness functions, are adequately protected against cyber attacks. This requirement to provide a cyber security plan (CSP) to the NRC for review is codified in Title 10 of the *Code of Federal Regulations* (CFR), Section 73.54, "Protection of Digital Computer and Communication Systems and Networks." Applicant/licensees must identify those assets that must be protected against cyber attacks; establish, implement, and maintain a cyber security program for the protection of the assets; and ensure that the cyber security program is incorporated into the physical protection program. The cyber security program must implement security controls to protect Critical Digital Assets (CDA) from cyber attacks, apply and maintain defense-in-depth protective strategies, mitigate the effects of cyber attacks, and ensure that the

functions of the CDAs are not adversely impacted by the cyber attacks. The cyber security program must include adequate training, evaluate and manage cyber risk, and ensure that the cyber security performance objectives for CDAs are maintained during modifications. The applicant/licensee must establish, implement, and maintain a CSP that implements the cyber security program requirements of 10 CFR 73.54. The applicant/licensee must develop and maintain written policies and procedures to implement the CSP. The applicant/licensee must review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The applicant/licensee must retain all records and supporting technical documentation required to satisfy the recordkeeping requirements of 10 CFR 73.54 until the Commission terminates the license for which the records were developed. The applicant/licensee must also maintain the superseded portions of such records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

The scope of the review is programmatic. The NRC staff does not review design information contained in the CSP.

Specific information to be reviewed, referenced to applicable sections of 10 CFR 73.54, includes the following:

1. the purpose and scope of the applicant/licensee's cyber security program (10 CFR 73.54(a))

2. the performance basis of the applicant/licensee's cyber security program (10 CFR 73.54(c) and 10 CFR 73.54(e))

3. a discussion of the licensee's formal, documented security planning, assessment, and authorization policy (10 CFR 73.54(f))

4. a discussion of the applicant/licensee's cyber security training (10 CFR 73.54(d)(1))

5. a discussion of the applicant/licensee's identification of CDAs (10 CFR 73.54(b)(1))

6. a discussion of the applicant/licensee's reviews and validation testing of critical systems (CS) and CDAs (10 CFR 73.54(b)(2))

7. the applicant/licensee's defense-in-depth protective strategies (10 CFR 73.54(c)(2))

8. a discussion of the application of security controls (10 CFR 73.54(c)(1))

9. a discussion of the incorporation of the cyber security program into the physical protection program (10 CFR 73.54(b)(3))

10. a discussion of policies and implementing procedures for the cyber security program (10 CFR 73.54(f))

11. a discussion of continuous monitoring and assessment (10 CFR 73.54(b)(2) and 10 CFR 73.54(d)(2))

12. a discussion of periodic assessment of security controls (10 CFR 73.54(b)(2) and 10 CFR 73.54(d)(2))

13. a discussion of effectiveness analysis (10 CFR 73.54(b)(2) and 10 CFR 73.54(d)(2))

14. a discussion of vulnerability assessments and scans (10 CFR 73.54(b)(2) and 10 CFR 73.54(d)(2))

15. a discussion of change control processes (10 CFR 73.54(d)(3))

16. a discussion of configuration management (10 CFR 73.54(d)(3), 10 CFR 73.54 (f), and 10 CFR 73.54 (g))

17. a discussion of the security impact analysis of changes (10 CFR 73.54(d)(3))

18. a discussion of security reassessment and authorization (10 CFR 73.54(d)(3))

19. a discussion of the updating of cyber security practices (10 CFR 73.54(f))

20. a discussion of the review and validation testing of a modification or addition of a CDA (10 CFR 73.54(d)(3))

21. a discussion of the application of security controls associated with a modification or addition (10 CFR 73.54(c)(1) and 10 CFR 73.54(d)(3))

22. a discussion of the cyber security program review (10 CFR 73.54(g))

23. a discussion of document control and records retention and handling (10 CFR 73.54(h))

Operational Program Description and Implementation

For a combined license (COL) application, the NRC staff reviews the CSP description and the proposed implementation milestones. The NRC staff also reviews the table of operational programs required by NRC regulations in the final safety analysis report (FSAR) to ensure that the CSP and associated milestone is included.

Review Interfaces

Other required Standard Review Plan (SRP) sections interface with this section as follows:

1. SRP Section 13.6, “Physical Security”

2. SRP Section 13.4, “Operational Programs” (For COL reviews of operational programs, the review of the applicant/licensee’s implementation plan is performed under this section.)

II. ACCEPTANCE CRITERIA

Acceptance criteria are based on meeting the relevant requirements of the following Commission regulations:

1. 10 CFR 73.54

2. 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), and 10 CFR 73.55(m)

3. Appendix G, “Reportable Safeguards Events,” to 10 CFR Part 73, “Physical Protection of Plants and Materials”

4. 10 CFR 73.58, “Safety/Security Interface Requirements for Nuclear Power Reactors”

Specific criteria acceptable to meet[1] the relevant requirements of the Commission’s regulations identified above are as follows for each review described in Section I of this SRP section:

The security plan is considered acceptable if it agrees with the plan template in Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," the most recent NRC-approved Nuclear Energy Institute (NEI) 08-09, "Cyber Security Plan for Nuclear Power Reactors," or any other NRC-approved set of guidelines.

1. As required by 10 CFR 73.54, an applicant/licensee or licensee must provide a high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat (DBT) described in 10 CFR 73.1, “Purpose and Scope.”

2. As required by 10 CFR 73.55(a)(1) and 10 CFR 73.55(b)(8), an applicant/licensee or licensee must submit a CSP and establish, maintain, and implement a cyber security program.

3. As required by 10 CFR 73.55(m)(2), an audit of the effectiveness of the cyber security program must be conducted.

4. Appendix G to 10 CFR Part 73 requires licensees to report or record, as appropriate, the following safeguards events:

    A. any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause:

        i. significant physical damage to a power reactor
        ii. interruption of normal operation of a licensed nuclear power reactor through the unauthorized use of or tampering with its machinery, components, or controls including the security system

    B. any failure, degradation, or the discovered vulnerability in a safeguard system that could allow unauthorized or undetected access to a protected area or vital area for which compensatory measures have not been employed.

    C. An actual entry of an unauthorized person into a protected area

    D. The actual or attempted introduction of contraband into a protected area

    E. any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to a protected area or vital area had compensatory measures not been established

[1] The SRP is not a substitute for the NRC’s regulations, and compliance with it is not required. However, in accordance with 10 CFR 50.34(h), an applicant/licensee is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria. The applicant/licensee must also evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

F. any other threatened, attempted, or committed act not previously defined in Appendix G to 10 CFR Part 73 with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness

5. As required by 10 CFR 73.58(b), licensees must assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security. The scope of changes to be assessed and managed must include planned and emergent activities (such as, but not limited to, physical modifications, procedural changes, changes to operator actions or security assignments, maintenance activities, system reconfiguration, access modification or restrictions, and changes to the security plan and its implementation). If potential conflicts are identified, the licensee must communicate them to appropriate licensee personnel and take compensatory or mitigative actions or both to maintain safety and security under applicable Commission regulations, requirements, and license conditions.

Operational Programs

For COL reviews, the NRC staff will review the description of the operational program and proposed implementation milestone for the CSP in accordance with 10 CFR 73.54. The implementation milestone occurs before fuel arrives on-site.

Technical Rationale

The following paragraphs discuss the technical rationale for applying these acceptance criteria to the review of this SRP section.

1. The NRC regulations at 10 CFR 73.54 include the cyber security program requirements for power reactor licensees. Subsequent to the events of September 11, 2001, the NRC issued orders to require power reactor licensees to implement measures to enhance cyber security. These security measures require an assessment of cyber systems and the implementation of corrective measures sufficient to provide protection against the cyber threats at the time the orders were issued. The requirements maintain the intent of the security order by establishing the requirement for a cyber security program to protect digital computer and communication systems and networks that, if compromised, can adversely impact SSEP. This includes support systems and equipment.

2. Recently, the NRC revised 10 CFR 73.55 to codify the cyber security requirements for NRC-licensed power reactors. In particular, 10 CFR 73.55(a)(1) and 10 CFR 73.55(b)(8) require that an applicant or licensee submit a CSP and establish, maintain, and implement a cyber security program. Finally, 10 CFR 73.55 requires an audit of the effectiveness of the cyber security program at least every 24 months.

3. Appendix G to 10 CFR Part 73 requires licensees to report or record, as appropriate, safeguards events. These events include cyber attacks.

4. As required by 10 CFR 73.58, licensees must assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

III. REVIEW PROCEDURES

The purpose of the review procedures is to determine whether a CSP is in line with the guidance in RG 5.71, the provisions of applicable NRC regulations, the information requirements of Section I above, and the acceptance criteria of Section II above. Table 1 provides a checklist for reviewers to use when reviewing the body of the CSP. Table 2 and Table 3 provide listings of security controls with time associations. Reviewers can use these for comparison with the frequencies in the CSPs being reviewed.

Table 1 - Acceptance Review Checklist for Cyber Security Plan Evaluation

Format and Content Guide	Requirement	Acceptance Criteria	Accept	Accept with RAI	Reject
RG 5.71	**Introduction**				
A.1	As required by 10 CFR 73.54(e) and 10 CFR 73.55(c)(6), licensees and applicant/licensees must establish, implement, and maintain a cyber security program for each site to protect digital computer and communication systems and networks from cyber attacks, up to and including the DBT described in 10 CFR 73.1.	Licensees and applicants must establish, implement, and maintain a cyber security program for each site. Licensees and applicants may comply with the requirements of 10 CFR 73.54 by implementing the guidance in RG 5.71.			
A.2	**Cyber Security Plan**				
A.2.1	Scope and Purpose				
	Required by 10 CFR 73.54(e), this plan describes how licensees and applicant/licensees will establish a cyber security program to achieve high assurance that digital systems, networks, and communication systems are protected.	The CSP describes the following: • implementation and documentation of the "baseline" security controls, as described in Regulatory Position C.3.3 of RG 5.71 • implementation and documentation that the cyber security program employs a life-cycle approach to maintain security controls, as described in Section Regulatory Position C.4. of RG 5.71.			

A.2.2	Performance-Based Requirements				
	A licensee must establish, implement, and maintain the CSP, as required by 10 CFR 73.55(e). As required by 10 CFR 73.54(b)(3), cyber security is a component of the physical protection program.	The CSP establishes how digital computer and communication systems and networks within the scope of 10 CFR 73.54 will be adequately protected from cyber attacks up to and including the DBT.			
A.3	**Cyber Security Program Implementation**				
	A licensee must establish, implement, and maintain a program that complies with the requirements of 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8) to protect systems within the scope of 10 CFR 73.54(a)(1).	The CSP complies with 10 CFR 73.54 as follows: • establishes and implements the defensive model described in Section 3.15 of this plan, with the security controls described in Sections C.3.1, C.3.2, and C.3.3 of RG 5.71 • maintains the program described in Section C.4 of RG 5.71 • ensures that documentation of security controls is available for each CDA for inspection • ensures that the NRC will approve any changes that decrease the effectiveness of the plan • ensures that reports of any cyber attacks or incidents at the site are made to the NRC as required by 10 CFR 73.71, “Reporting of Safeguards Events” and Appendix G, “Reportable Safeguards Events,” to 10 CFR Part 73, “Physical Protection of Plants and Materials.”			

A.3.1	Analyzing Digital Computer Systems				
A.3.1.1	Security Assessment and Authorization				
	As required by 10 CFR 73.54(f), licensees must develop and maintain policies and procedures to implement the CSP.	The CSP discusses the following policies and procedures: • a formal documented security planning, assessment, and authorization policy that describes the purpose, scope, roles, responsibilities, management commitments, and coordination among departments and the implementation of the security program and the controls listed in Appendices B and C of RG 5.71 • a formal documented procedure to facilitate the implementation of the cyber security program and the security assessment			

A.3.1.2	Cyber Security Team				
	In order to comply with 10 CFR 73.54(c)(2), licensees should establish and maintain defense in depth protective strategies.	It is advised that the CST should have the authority to conduct an objective assessment, make determinations, implement the defense-in-depth protective strategies, and implement the security controls using the process in Section C.3.3 of RG 5.71. It is recommended that the CST must have broad knowledge in the following areas: • information and digital system technology: – cyber security – software development – communications – systems administration – computer engineering – networking — site and corporate networks – programmable logic controllers – control systems – distributed control systems – computer systems and databases used in design, operation, and maintenance of CDAs • nuclear facility operations, engineering and technical specifications • physical security and emergency preparedness systems and programs			

	In order to comply with 10 CFR 73.54(d)(1), the CST should have particular roles and responsibilities.	The submitted CSP lists the roles and responsibilities for the CST, which include the following: • Perform or oversee each stage of cyber security management processes. • Document all key observations, analyses, and findings during the assessment process so that information can be used in the application of security controls. • Evaluate or reevaluate assumptions or conclusions about current cyber security threats. • Evaluate or reevaluate assumptions or conclusions about potential vulnerabilities to, and consequences from, an attack. • Evaluate or reevaluate assumptions or conclusions about the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; and cyber security awareness and training of those working with, or responsible for, CDAs and cyber security controls throughout their system life cycles. • Confirm information from reviews of CDAs and connected digital devices and associated security controls with physical and electronic validation activities.			

		• As needed, identify and implement new cyber security controls. • Document the implementation of alternate or compensating measures in lieu of any security controls (Appendices B and C of RG 5.71). • Document the basis for not implementing certain controls (Appendix B to RG 5.71). • Prepare documentation and oversee implementation of security controls (Appendices B and C to RG 5.71). • Retain all documentation in accordance with 10 CFR 73.55(q) and Section C.5 of RG 5.71.			
	As required by 10 CFR 73.54(d)(2), the CST conducts objective security assessments to evaluate and manage cyber risks.	Security assessment determinations are not constrained by operational goals.			

A.3.1.3	Identification of CDAs				
	As required by 10 CFR 73.54(b)(1), the licensee must identify and document each CDA that has a direct, supporting, or indirect association with the proper functioning of CS.	The submitted CSP provides a description of methods that: • identify and document systems, equipment, communication systems, and networks that are associated with the SSEP functions described in 10 CFR 73.54(a)(1), as well as the support systems associated with these SSEP functions. Systems, equipment, and network systems associated with SSEP functions are referred to as CS. The CST identifies CS by conducting an initial consequence analysis of systems, equipment, communication systems, and networks to determine those which, if compromised, exploited, or failed, could impact the SSEP functions of the nuclear facility, without taking into account existing mitigating measures. • perform a dependency and pathway analysis of any system or equipment associated with SSEP functions to determine whether they are CS. • identify and document CDA that have a direct, supporting, or indirect role in the proper functioning of CS.			

	As required by 10 CFR 73.54(b)(1), the licensee must examine each CS and document the results.	The submitted CSP discusses the means to document the following: • description of CDA • identification of each CDA within each CS • description of CDA functional(s) • identification of the consequences to the CS and SSEP functions, if a compromise were to occur • identification of the digital devices having direct or indirect roles in CS function • description of security functional requirements or specifications that includes: – security requirements for vendor or developers to maintain system integrity – secure configuration, installation, and operation of the CDA – effective use and maintenance of security features or functions – known vulnerabilities regarding configuration and use of administrative functions – effective use of user-accessible security features or functions – methods for user interaction with CDA – user responsibilities in maintaining the security of the CDA			

A.3.1.4	Reviews and Validation Testing				
	As required by 10 CFR 73.54(e)(1), the CSP must describe implementation of the program and address site-specific conditions.	The submitted CSP states that CST conducted a review and performed validation activities and for each CDA— • direct/indirect connection pathways • infrastructure interdependencies • application of defensive strategies, including defensive models, security controls, and other defensive measures			

	In order to comply with 10 CFR 73.54(e)(1), the CST should validate the above activities with a walkdown.	The walkdown includes the following: • performing physical inspection of the connections and configuration of each CDA • for each CDA, tracing all communication connections into and out of each termination point along the pathway • examining the physical security of the CDA including the communication pathways • examining the configuration and assessing the effectiveness of existing security controls along the communication pathways • examining interdependencies for each CDA and trust relationships and between CDAs • examining interdependencies with infrastructure support systems emphasizing compromises of electrical power, environmental controls, and fire equipment • examining systems, communication systems, and networks that are potential pathways for attacks • resolving discrepancies found in the review			

	In order to comply with 10 CFR 73.54(e)(1), the CST should perform electronic validations as appropriate.	An electronic validation is performed when a walkdown inspection is impractical and consists of tracing a communication pathway from start to finish. Use of electronic equipment may prove a better method than a physical walkdown.			
A.3.1.5	Defense-in-Depth Protective Strategies				
	As required by 10 CFR 73.54(c)(2), licensees must apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks.	The submitted CSP provides for the implementation of defensive strategies that ensure the capability to detect, respond to, and recover from a cyber attack. The defensive strategies consist of the following: • security controls implemented in accordance with Section 3.1.6 of the CSP and the defense model outlined in Regulatory Position C.3.2 of RG 5.71 • defense-in-depth measures described in Section 6 of Appendix C to RG 5.71 • detailed defensive architecture described in Section 7 of Appendix C to RG 5.71 • maintenance of a cyber security program in accordance with Section 4 of Appendix A to RG 5.71 The defense model establishes the logical and physical boundaries between CDAs with similar risks and CDAs with lower security risks.			

A.3.1.6	Application of Security Controls				
	As required by 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(2), the licensee must design its cyber security program with defense-in-depth, including implementation of security controls to protect CDAs from cyber attacks.	The licensee establishes defense-in-depth strategies by implementing and documenting the following: • defensive model (Section C.3.2 of RG 5.71) • physical security program and physical barriers • operational and management controls described in Appendix C to RG 5.71 • technical controls described in Appendix B to RG 5.71			

	Technical Security Controls				
		The submitted CSP discusses using the information collected from Section 3.1.4 of the CSP to conduct one or more of the following: 1. Implement all security controls specified in Appendix B to RG 5.71. 2. If a security control cannot be applied, implement an alternative control listed in Appendix B to RG 5.71 by doing one of the following: A. Document the basis for the countermeasure. B. Perform and document an attack vector/tree analysis of the CDA to confirm that the countermeasure provides the same or greater protection as the corresponding control. 3. Do not implement a control enumerated in Appendix B to RG 5.71 and— A. Perform an attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented. B. Document that the attack vector does not exist and demonstrate that the control is not necessary.			

	As required by 10 CFR 73.58(b), 10 CFR 73.58(c), and 10 CFR 73.58(d), the licensee must address adverse impacts of security controls.	The submitted CSP notes that, before implementing security controls on a CDA, the potential for adverse impact must be assessed. Specifically, the licensee— • should not implement a security control if there is a known adverse impact to SSEP functions • should use alternate controls to mitigate the lack of the security control, in accordance with Section 3.1.6 of the CSP			
	In order to comply with 10 CFR 73.54(c)(2) Licensees should perform effectiveness analysis, vulnerability assessments, and scans	The submitted CSP includes provisions to verify that CDAs are adequately protected from cyber attacks up to and including the DBT and that any identified gaps have been closed. The program should recommend the licensee do the following: • Perform an effectiveness analysis, as described in Section C.4.1.2 of RG 5.71. • Perform a vulnerability assessment or scans, as described in Section C.4.1.3 of RG 5.71.			

A.3.2	Incorporating the Cyber Security Program into the Physical Protection Program				
	The licensee must follow the provisions of 10 CFR 73.54(b)(3), 10 CFR 73.55(a)(1), 10 CFR 73.55(c)(6), and 10 CFR 73.55(f)(2).	The CSP discusses the following efforts necessary to integrate the management of physical and cyber security: • establishment of a security organization, independent from operations, to incorporate both cyber and physical security • documentation of physical and cyber security interdependencies • development of policies and procedures joining management, physical, and cyber security controls • incorporation of policies and procedures to secure the CDAs from attacks up to and including the DBT • coordination of the acquisition of physical or cyber security services, training, devices, and equipment • coordination of personnel training • integration and coordination of incident response personnel • training of senior management • performance of periodic exercises of simulated physical and cyber attacks			

A.3.3.	Policies and Implementing Process				
	As required by 10 CFR 73.54(f), the licensee must develop and maintain policies and procedures to implement the CSP.	The CSP states the following: • The licensee is advised to develop and implement policies and procedures to meet the security control objectives provided in Appendices B and C to RG 5.71. • The licensee is advised to document, review, approve, issue, use, and revise policies and implementation procedures as described in Section 4 of the CSP. • The licensee is advised to ensure personnel responsible for implementing and overseeing the program report to an executive who is responsible for nuclear plant operation. • It is recommended that licensee's procedures establish specific responsibilities for positions described in Section C.10.10 of RG 5.71.			

A.4	**Maintaining the Cyber Security Program**				
	As required by 10 CFR 73.54(b)(2), the licensee must implement the elements in this section to adequately protect the site from cyber attacks.	The CSP states the following: • The licensee will employ a life-cycle approach consistent with the controls described in Appendix C of RG 5.71. • The licensee needs to maintain security controls for CDAs to achieve the overall cyber security program objectives. • For new or existing CDAs undergoing modifications, the licensee should follow the process described in Section 4.2 of the CSP.			
A.4.1	Continuous Monitoring and Assessment				
	In order to comply with 10 CFR 73.54(b)(2), 10 CFR 73.54(d)(2), and 10 CFR 73.54(e)(2), the licensee should monitor the controls described in Appendix C to RG 5.71. Automated support tools are used for near real-time cyber management for CDAs.	The CSP describes a continuous monitoring program, including the following: • ongoing assessments to verify that security controls remain in place throughout the life cycle • verification that rogue assets have not been connected to the infrastructure • periodic assessment to verify effectiveness and need for the security controls described in Appendices B and C to RG 5.71 • periodic security program review to evaluate and improve the effectiveness of the program • support for configuration management • possible updates to the CSP			

A.4.1.1	Periodic Assessment of Security Controls				
	As required by 10 CFR 73.54(b)(2) and 10 CFR 73.54(d)(2), the licensee must maintain the cyber security program and evaluate and manage cyber risks.	The CSP states the following: • The licensee must perform periodic assessments to verify that the security controls implemented for each CDA remain robust, resilient, and effective. • The CST must verify the status of the controls annually or in accordance with the guidance described in Appendices B and C to RG 5.71, whichever is more frequent.			
A.4.1.2	Effectiveness Analysis				
		The CSP states the following: • The CST monitors and measures the cyber security program and security controls to ensure that the controls were implemented correctly and are operating as intended, thus assuring protection against cyber attacks. • Licensee reviews of the security program and controls include periodic testing of the security controls and re-evaluation of adversary capabilities. • Licensee reviews of the security program and controls include audits of the following: – physical security program and implementing procedures – safety/security interface activities – testing, maintenance, and calibration programs – operating experience			

		program • The licensee considers feedback from the NRC and law enforcement agencies. • The CST verifies the effectiveness of security controls annually or in accordance with Appendices B and C to RG 5.71. • The CST reviews records of maintenance and repairs to ensure that security functions are maintained in accordance with recommendations provided by the manufacturer.			
		The insights gained from these analyses are used to: • improve performance and effectiveness of the cyber security program, • manage and evaluate risk, • improve the effectiveness of implemented security controls described in Appendices B and C to RG 5.71, • ascertain whether new security controls are required to protect CDAs from cyber attack, • verify that existing security controls are functioning properly and are effective at protecting CDAs from cyber attack, and • facilitate corrective action of any gaps discovered in the security program.			

A.4.1.3	Vulnerability Assessments & Scans				
	As required by 10 CFR 73.54(b)(2) and 10 CFR 73.54(d)(2), the licensee must maintain the cyber security program and evaluate and manage cyber risks.	The CSP states the following: • The licensee will conduct vulnerability scans or assessments, identify deficiencies, and resolve the deficiencies. The frequency of the scans and assessments is at least once each quarter. Refer to RG 5.71, Appendices B and C, for frequency for specific controls. • The CST will perform vulnerability scans or assessments when new vulnerabilities that could potentially affect the effectiveness of the controls are identified. • The CST will employ up-to-date vulnerability scanning tools and techniques. • The CST will evaluate scan and assessment reports and address vulnerabilities that could adversely impact SSEP functions. • The CST will share scanning and assessment information with appropriate personnel to ensure that vulnerabilities that may affect similar or inter-connected CDAs or impact the effectiveness of the CDA functions or the SSEP functions or both are understood, evaluated, and mitigated.			

		• The CST will ensure that the assessment and scanning does not adversely impact SSEP functions. If an impact is detected, the CDA will be removed from service or replicated before assessment and scanning is conducted. • If the Licensee/Applicant cannot conduct vulnerability assessments or scanning on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls (e.g., providing a replicated system or CDA to conduct scanning) will be employed.			

A.4.2	Change Control				
	As required by 10 CFR 73.54(d)(3), the licensee must ensure that modifications are evaluated to ensure that cyber security objectives are met.	The CSP states the following: • It is advised that the licensee/applicant will systematically plan, approve, test, and document changes to the environment of a CDA. • Changes to existing CDAs or addition of a new CDA must be made in a manner that ensures that the SSEP functions are protected from a cyber attack. • During the operation and maintenance life-cycle phases, the program establishes that changes made to CDAs, design control and configuration management procedures or other procedural processes ensure that the existing security controls are effective and that any pathway that can be exploited to compromise a CDA is protected from cyber attacks. • During the retirement phase, the design control and configuration management procedures or other procedural processes address safety, reliability, and security engineering activities.			

A.4.2.1	Configuration Management				
	In order to comply with 10 CFR 73.54(d)(3), 10 CFR 73.54(f), and 10 CFR 73.54(g), licensees should ensure that modifications to critical digital assets, are evaluated before implementation to ensure that the cyber security performance are maintained.	The CSP states the following: • It is advised that the licensee will implement and document the configuration management controls described in Section C.11 of RG 5.71. • The licensee will implement a configuration and change management system as described in Section C.11 of RG 5.71. • Before modifications are implemented, the licensee must evaluate them using the criteria in Section 4.2 of the CSP to ensure that the performance objectives identified in 10 CFR 73.54(a)(1) are maintained.			

A.4.2.2	Security Impact Analysis of Changes and Environment				
	In order to comply with 10 CFR 73.54(d)(3), the security impact analysis should assist in managing potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats.	The CSP states the following: • It is advised that the CST will perform a security impact analysis in accordance with CSP Section 4.1.2 before implementing a design or configuration change or when changes to the environment occur. • The CST will evaluate, document, and incorporate into the security impact analysis the safety and security interdependencies of other CDAs or systems. The CST will also update and document the following: – location of CDA and connected assets – connectivity pathways – infrastructure interdependencies – application of defensive strategies including: ◦ defensive models ◦ security controls ◦ other defensive strategy measures – plant-wide physical and cyber security policies and procedures, including attack mitigation and incident response and recovery • The licensee will perform impact analyses as part of the change approval process and address identified gaps to protect CDAs from attack as described in Section 4.2.6 of this plan.			

		• The licensee will manage the cyber security of SSEP functions and CDAs through ongoing evaluation, as described in Appendices B and C to RG 5.71, during all phases of the life cycle. • The licensee will establish procedures for screening, evaluating, mitigating, and dispositioning threat and vulnerability notifications received from credible sources. This includes implementation of security controls to mitigate new issues.			
A.4.2.3	Modification of CDAs				
	As required by 10 CFR 73.54(d)(3), the licensee must ensure that modifications to CDAs are evaluated before implementation.	It is recommended that the licensee must disseminate, review, and update the following when a CDA modification is conducted: • documented security assessment and authorization policy to reflect all modifications • documented procedure to facilitate the implementation of the security reassessment and authorization policy and associated controls			

A.4.2.4	Updating Cyber Security Practices				
	In order to comply with 10 CFR 73.54(e), the CST should update the cyber security practices.	It is advised that the CST review, update, and modify information on cyber security policies, procedures, practices, existing cyber security controls, network architecture, security devices, and any other information associated with the state of the security program or security controls provided in Appendices B and C to RG 5.71 when changes occur to a CDA or the environment. This information includes the following: • detailed network architectures and diagrams • configuration information on security devices or CDAs • new plant or corporate-wide cyber security defensive strategies or security controls being developed and policies, procedures, practices, and technologies related to their deployment • the site's physical and operational security program • cyber security requirements for vendors and contractors • identified potential pathways for attacks • recent cyber security studies or audit results • identified infrastructure support systems whose failure or manipulation could impact the proper functioning of CS			

A.4.2.5	Review and Validation Testing of Modification or Addition of a CDA				
	In order to comply with 10 CFR 73.54(d)(3), the CST should document the results of reviews and validation tests.	The CST documents the results of reviews and validation tests of each CDA modification and addition using the process described in Regulatory Position C.3.1.4 of RG 5.71.			
A.4.2.6	Application of Security Controls Associated with a Modification or Addition				
	As required by 10 CFR 73.54(c)(1) and 10 CFR 73.54(d)(3), the licensee must apply security controls associated with modifications.	The licensee undertakes the following when new CDAs are introduced: • deploys the CDA into the appropriate level of the defensive model described in Section 3.1.5 of this plan, • applies the technical controls identified in Appendix B to RG 5.71 in a manner consistent with the process described in Section 3.2 of RG 5.71, and • confirms that the operational and management controls described in Appendix C of RG 5.71 are applied and effective for the CDA.			

A.4.3	Cyber Security Program Review				
	The cyber security program establishes the necessary measures and procedures to implement periodic reviews of applicable program elements, in accordance with the requirements of 10 CFR 73.55(m) and 10 CFR 73.54(g).	The licensee conducts reviews as follows: • the program's effectiveness at least every 24 months • within 12 months of initial implementation of program • within 12 months of a change to personnel, procedures, equipment, or facilities that could adversely affect security • as necessary based upon site-specific analyses, assessments, or other performance indicators • by individuals independent of those personnel responsible for program implementation and management The licensee documents the results and recommendations of program reviews, management findings, and any actions taken as a result of recommendations from prior program review. The licensee generates a report to the site's plant manager and to the site's corporate management at least one level higher than the individual having responsibility for day-to-day plant operation. The licensee maintains these reports in an auditable form, available for inspection, and enters findings from program reviews into the site's Corrective Action Program.			

A.5	**Document Control and Records Retention and Handling**				
	As required by 10 CFR 73.54(h), the licensee must establish and implement a cyber security document control and records policy and related procedures.	The CSP states the following: • The licensee establishes the necessary measures and procedures to ensure that records of items and activities are developed, reviewed, approved, issued, used, and revised to reflect completed work affecting cyber security. • The licensee retains records and supporting documentation required to satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55 until the NRC terminates the facility operating license. Records required for retention include, but are not limited to, all digital records, log files, audit files, and non-digital records that capture, record, and analyze network and CDA events. The licensee retains these records to document access history and discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions or both. • The licensee retains superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the NRC.			

Table 2 - Regulatory Guide 5.71, Appendix B, Technical Security Controls

(This table contains only those technical controls with time associations. To aid the reviewer, the description of the periodicity of these controls has been expanded beyond that which is provided in RG 5.71.)

B.1.1 Access Control Policy and Procedure	
	• Develop, disseminate, and annually review and update a formal, documented CDA and CS access control policy which addresses the purpose, scope, roles, responsibilities, management commitments, and internal coordination of such policy. • Audit CDAs annually or immediately upon changes in personnel responsibilities or major changes in system configurations or functionality.
B.1.2 Account Management	
	• Review CDA/CS accounts in a manner consistent with the access control list provided in the design control package, access control program, and cyber security procedures. Initiate required actions on CDA/CS accounts no less frequently than once every 30 days. • Review and document CDA/CS accounts at a maximum interval consistent with the most recent version of NEI 03-12, "Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan," endorsed by the NRC for CDAs/CS in vital areas and CDAs/CS that provide security functions protecting vital areas. • Employ automated mechanisms that support CDA/CS account management functions and enable CDAs/CS to: – terminate temporary, guest, and emergency accounts no less frequently than once every 30 days – disable inactive accounts no less frequently than once every 30 days – document and immediately notify system administrators of all account creation, deletion, and modification activities to ensure that administrators are aware of any account modifications and can investigate potential cyber attacks

B.1.7 Unsuccessful Login Attempts	
	• Implement security controls to limit the number of invalid access attempts by a user. Document this requirement in the access control policy. The number of failed login attempts in a specified time period may vary by CDA/CS. For example, the licensee may implement a security control that will automatically lock out the account after more than three invalid login attempts are made within a 1-hour time period. The licensee's system enforces the lock out mode automatically. • The access control policy includes a requirement that only authorized individuals, who are not the user, can unlock accounts once the maximum number of unsuccessful login attempts has been exceeded. Alternatively, other verification techniques or mechanisms that incorporate identity challenges may be used.
B.1.10 Session Lock	
	Configure CDAs/CS to do the following: • Initiate a session lock after 30 minutes of inactivity. • Implement alternative controls and document the justification for alternative controls or countermeasures for those instances in which a CDA/CS cannot support session locks. • Monitor and record physical access to the CDA/CS to detect and respond to intrusions immediately.
B.1.17 Wireless Access Restrictions	
	Conduct scans no less frequently than once every week for unauthorized wireless access points, in accordance with this document, and disable access points if unauthorized access points are discovered.
B.1.18 Insecure and Rogue Connections	
	Verify that, during deployment of CDAs/CS, when changes or modifications have been made to CDAs/CS, and no less frequently than once every month, CDAs/CS are free of insecure (i.e., rogue) connections, such as vendor connections and modems.
B.2.1 Audit and Accountability Policy and Procedures	
	Develop, disseminate, and annually review and update the following while using an independent party for the audit reviews: • a formal, documented audit and accountability policy that addresses the purpose, scope, roles, responsibilities, management commitments, and internal coordination of the policy • a formal, documented procedure that facilitates the implementation of the audit and accountability policy and associated audit and accountability security controls

B.2.2 Auditable Events	
	Review and update the list of defined auditable events no less frequently than once a year.
B.2.5 Response to Audit Processing Failures	
	CDAs provide a warning when the allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity, which is based on the function of how quickly storage capacity is consumed and the organization's resources and response times (e.g., 60 to 70 percent of storage capacity).
B.2.6 Audit Review, Analysis, and Reporting	
	Review and analyze the CDA/CS audit records no less frequently than once every 30 days for indications of inappropriate or unusual activity and report findings to designated official.
B.3.1 Critical Digital Asset/Critical System and Communications Protection Policy and Procedures	
	Develop, disseminate, and annually review and update the following: • a formal, documented CDA/CS system and communications protection policy that addresses the purpose, scope, roles, responsibilities, management commitments, and internal coordination of the system • a formal, documented procedure that facilitates the implementation of the CDA/CS system and communications protection policy and associated CDA/CS system and communications protection security controls
B.4.1 Identification and Authentication Policies and Procedures	
	The identification and authentication policy and procedures provide guidance on managing both user identifiers and CDA/CS authenticators. These items include the following: • disable user identifier after a maximum of 30 days of inactivity • annual changing or refreshing of authenticators
B.4.3 Password Requirements	
	Change passwords periodically (e.g., every 30 days for workstations; every 3 months for CDAs in a vital area).
B.4.6 Identifier Management	
	Manage and document user identifiers by disabling the user identifier after a maximum of 30 days of inactivity.
B.4.7 Authenticator Management	
	Manage CDA/CS authenticators by changing/refreshing authenticators annually.

Table 3 - Regulatory Guide 5.71, Appendix C,
Management and Operations Security Controls

(This table contains only those management and operations controls with time associations. To aid the reviewer, the description of the periodicity of these controls has been expanded beyond that which is provided in RG 5.71.)

C.1.1 Media Protection Policy and Procedures	
	The licensee develops, disseminates, and annually reviews and updates the following: • a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among site entities, and compliance for each information category, as defined by the site policies, and ensures that any media which can provide information to assist an adversary is marked at a minimum to identify the sensitive nature of the media • a formal, documented procedure to facilitate the implementation of the media protection policy and all associated media protection controls, including the methodology that defines the purpose, scope, roles, responsibilities, and management commitments in the areas of media receipt, storage, handling, sanitization, removal, reuse, and disposal necessary to provide high assurance that the risk of unauthorized disclosure of information that could be used in a cyber attack to adversely impact the SSEP functions of the nuclear facility is prevented
C.1.6 Media Sanitation and Disposal	
	The licensee tracks, documents, and verifies media sanitization and disposal actions and performs quarterly tests on sanitized data to ensure that equipment and procedures are functioning properly.
C.3.1 System and Information Integrity Policy and Procedures	
	The licensee develops, disseminates, and annually reviews and updates the following: • a formal documented system and information integrity policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among licensee entities, and compliance • formal documented procedures to facilitate the implementation of CDAs and an information integrity policy and associated system and information integrity controls
C.3.4 Monitoring Tools and Techniques	
	The licensee tests cyber intrusion detection and prevention systems, consistent with the timeframe defined in NEI 03-12, Section 20.1, for intrusion detection systems, and before being placed back in service after each repair or inoperative state.

C.3.5 Security Alters and Advisories	
	The licensee is responsible for the following: • receiving timely security alerts, bulletins, advisories, and directives from credible external organizations, as designated by the NRC and the licensee on an ongoing basis, such as third-party security alert notification services and vendor security alert lists, and maintaining a copy of these documents • independently evaluating and determining the need, severity, methods, and timeframes for implementing security directives consistent with the security controls for the CDA (Section 3.1 of Appendix A to RG 5.71) • within established timeframes set by the licensee or as directed by the NRC
C.3.7 Software and Information Integrity	
	The licensee reassesses and documents the integrity, operation, and functions of software and information by performing regular integrity, operation, and functional scans consistent with manufacturer or vendor recommendations, either quarterly, or as defined in NEI 03-12, or as required by NRC regulation, whichever is more frequent.
C.7 Defense in Depth	
	The licensee implements and documents security boundary control devices between higher security levels and lower security levels that include, except in the case of data diodes, a rule set that at a minimum is updated quarterly.
C.8.3 Incident Response Testing and Drills	
	The licensee is responsible for testing and conducting drills of the incident response capability for CDAs at least annually.
C.9.1 Contingency Planning Policy and Procedure	
	The licensee develops, disseminates, and annually reviews and updates the following: • a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among licensee entities, and compliance • formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls

C.9.3 Contingency Plan Testing	
	The licensee is responsible for conducting tests or exercises or both and documenting the contingency plan at least annually to verify its effectiveness and the organization's readiness to execute this plan.
C.9.4 Contingency Plan Training	
	The licensee is responsible for training personnel in their contingency roles and responsibilities with respect to the CDAs and providing refresher training at least annually or consistent with the licensee's overall contingency program, whichever period is shorter.
C.9.6 Critical Digital Asset Backups	
	The licensee is responsible for the following: • testing and documenting backup information monthly to verify media reliability and information integrity • establishing and documenting the timeframe in which data or the CDA must be restored and the frequency at which critical data and configurations are changing
C.11.2 Configuration Management Policy and Procedures	
	The licensee develops, disseminates, and annually reviews and updates formal, documented configuration management policy and implementing procedures that address the purpose, scope, roles, responsibilities, management commitment, coordination among licensee entities, associated configuration management controls, and compliance.
C.11.3 Baseline Configuration	
	The licensee documents the up-to-date baseline configurations and audits the configurations quarterly. Baseline configurations include but are not limited to a current list of all components (e.g., hardware, software), configuration of peripherals, version releases of current software, and switch settings of machine components. The licensee defines the minimum physical and logical access for the modifications. Additionally, the licensee employs electronic means to monitor CDA access to ensure that only authorized systems and services are used. The licensee also documents the justification for the use of alternate (compensating) security controls for instances in which monitoring cannot be done electronically, including the following: • physically restricting access • monitoring and recording physical access to enable immediate detection and response to intrusions • employing auditing and validation measures (e.g., security officer rounds, periodic monitoring of tamper seals) The licensee reviews log records no less frequently than once a quarter in compliance with the physical security plan.

C.11.6 Access Restrictions for Change	
	The licensee defines, documents, approves, and enforces physical and logical access restrictions associated with changes to CDAs and generates, retains, and audits the record quarterly and when there are indications that unauthorized changes may have occurred.
C.11.8 Least Functionality	
	The licensee reviews CDAs monthly to identify and eliminate unnecessary functions, ports, protocols, and services.
C.12.1 System and Services Acquisition Policy and Procedures	
	The licensee develops, disseminates, and annually reviews and updates a formal, documented system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among licensee entities, associated system and service acquisition controls, and compliance. The licensee develops, disseminates, and annually reviews and updates formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
C.12.6 Licensee/Applicant Testing	
	The licensee requires annual audits of CDAs to verify the following: • The security controls present during testing remain in place and are functioning correctly in the production system. • CDAs are free from known vulnerabilities and security compromises and continue to provide information on the nature and extent of compromises, should they occur. • The change management program is functioning effectively and is recording configuration changes appropriately.

C.13.1 Threat and Vulnerability Management	
	The licensee does the following: • performs assessments and scans for vulnerabilities in CDAs at least once each quarter and at random intervals in accordance with Section 4.1.3 of Appendix A to RG 5.71 and when new potential CDA vulnerabilities are reported or identified • analyzes vulnerability scan reports and remediates vulnerabilities immediately to provide a high degree of assurance that CDAs/CS are protected from cyber attacks up to and including the DBT • employs vulnerability scanning tools that include the capability to update the list of cyber vulnerabilities scanned and updates the list of CDA vulnerabilities scanned monthly and when new vulnerabilities are identified and reported • employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in CDA vulnerabilities and mitigation/flaw remediation activities • ensures that SSEP functions are not adversely impacted by scanning

The following additional guidance for the reviewer is provided:

- For reviews of CSPs for a new reactor, a table in FSAR Chapter 13 provides the implementation schedule, along with the implementation schedules for all other operational programs. The NRC will inspect the implementation of this program in accordance with NRC Inspection Manual Chapter IMC-2504, "Construction Inspection Program—Non-ITAAC Inspections." The reviewer will ensure that the program and associated implementation milestones are included within the license condition on operational program implementation.

- For reviews of CSPs for an operating reactor, the implementation schedule must consider refueling outages.

- For reviews of CSPs the phrase "cyber attack" must be defined in the CSP as "Any event in which there is a reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a CDA." See ADAMS Accession No. ML101550052.

IV. EVALUATION FINDINGS

The reviewer should verify that the applicant/licensee has provided sufficient information and that the review and calculations (if applicable) support conclusions of the following type to be included in the NRC staff's safety evaluation report. The reviewer should also state the bases for those conclusions.

The evaluation findings for a CSP review should be substantially equivalent to the following statement:

> A CSP has been submitted to demonstrate that the cyber security program will provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the DBT described in 10 CFR 73.1. The CSP has been withheld from public disclosure in accordance with the provisions of 10 CFR 2.390(d)(1).
>
> The applicant/licensee described the cyber security program based on the requirements of 10 CFR 73.54, including the audit of the effectiveness of the cyber security program at least every 24 months, as required by 10 CFR 73.55(m); safety and security interface, as required by 10 CFR 73.58; and reporting requirements, as required by Appendix G to 10 CFR Part 73. The implementation milestones for this program are included within the license condition on program implementation.
>
> The CSP has been reviewed for format and content utilizing the NRC CSP template, found to contain all features considered essential of such a program by the NRC staff, and is acceptable. In particular, it has been found to comply with the Commission's regulations, including 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), 10 CFR 73.55(m), 10 CFR 73.58, and Appendix G to 10 CFR Part 73, and it conforms to the applicable regulatory positions set forth in RG 5.71.

For COL reviews, the following license condition for operational programs should be added to the license:

> The applicant/licensee described the CSP and its implementation in conformance with 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), 10 CFR 73.55(m), 10 CFR 73.58, and Appendix G to 10 CFR Part 73. The license condition on operational program implementation includes the program and its implementation milestones.

V. IMPLEMENTATION

The following provides guidance to applicants and licensees regarding the NRC staff's plans for using this SRP section.

The NRC staff will use this SRP section when reviewing the CSP submittals of license amendment applications and license applications submitted by applicant/licensees in accordance with 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Except when the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the NRC staff will use the method described herein to evaluate conformance with Commission regulations.

The provisions of this SRP section apply immediately to reviews of applications to accommodate license amendment and COL application schedules.

VI. REFERENCES

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

2. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Chapter I, "Energy."

3. 10 CFR Part 73, "Physical Protection of Plants and Materials," Chapter I, "Energy."

4. NRC, "Power Reactor Security Requirements Final Rule" *Federal Register,* Vol. 74, No. 58, March 27, 2009, pp. 13926–13993.

5. NEI, "Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan," NEI 03-12, Revision 6.

6. NRC, "Cyber Security Programs for Nuclear Facilities," RG 5.71.

7. NRC, "Construction Inspection Program—Non-ITAAC Inspections," NRC IMC-2504.

SRP Section 13.6.6
"Cyber Security Plan"
Description of Changes

SRP Section 13.6.6 is a new section not previously included in NUREG-0800. It was developed to provide guidance for the review of CSPs.