U.S. NUCLEAR REGULATORY COMMISSION August 2016
OFFICE OF NUCLEAR REGULATORY RESEARCH Division 5

DRAFT REGULATORY GUIDE

Technical Lead
James Downs

DRAFT REGULATORY GUIDE DG-5062

(Proposed New Regulatory Guide)

Cyber Security Programs for Nuclear Fuel Cycle Facilities

A. INTRODUCTION

Purpose

This new regulatory guide (RG) describes methods and procedures that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for establishing, implementing, and maintaining a cyber security program at a nuclear fuel cycle facility (FCF) licensee subject to the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.53, "Requirements for cyber security at nuclear fuel cycle facilities." This RG describes an acceptable approach for meeting the cyber security performance objectives to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. This RG also provides guidance on the development of a cyber security plan and examples for establishing consequence of concern specific cyber security controls. A FCF licensee may use methods and standards other than those described within this RG to meet the Commission's regulations if the chosen measures and standards satisfy the stated regulatory requirements.

Applicability

This RG provides guidance for establishing, implementing, and maintaining a cyber security program at a nuclear fuel cycle facility under 10 CFR, Section 73.53, "Requirements for cyber security at nuclear fuel cycle facilities."

Applicable Regulations

The regulations in 10 CFR Part 73, "Physical Protection of Plants and Materials," Section 73.53, "Requirements for cyber security at nuclear fuel cycle facilities" apply to each applicant or licensee (hereinafter, the applicant and the licensee will be referred to collectively as "the licensee") subject to the requirements of 10 CFR 70.60, "Applicability," and licensees for conversion or deconversion of uranium hexafluoride licensed under 10 CFR Part 40, "Domestic Licensing of Source Material."

- Section 40.31(n) requires each application for a license to possess source material at a facility for the production, conversion or deconversion of uranium hexafluoride must include a cyber security plan that demonstrates how the applicant plans to meet the requirements of 10 CFR 73.53.

- Section 40.32(h) requires that the licensee make no change which would decrease the effectiveness of the cyber security plan prepared pursuant to 10 CFR 40.31(n) without the prior approval of the Commission. A licensee desiring to make such a change shall submit an

application for an amendment to its license pursuant to 10 CFR 40.44. The licensee may make changes to the cyber security plan without prior Commission approval if these changes do not decrease the effectiveness of the plan. The licensee shall retain a copy of the cyber security plan and maintain records of changes to the plan made without prior Commission approval, for three years from the effective date of the change, and shall, within two months after the change is made, furnish a report containing a description of each change to the Director, Division of Security Policy, Office of Nuclear Security and Incident Response; the report may be sent using an appropriate method listed in 10 CFR 70.5(a), and a copy of the report must be sent to the appropriate NRC Regional Office shown in appendix A to part 73 of this chapter.

- Section 70.22(o) requires each application for a license to possess or use at any site or contiguous sites subject to licensee control, a formula quantity of strategic special nuclear material or special nuclear material of moderate strategic significance or 10 kg or more of special nuclear material of low strategic significance as defined under 10 CFR 70.4, other than a license for possession or use of this material in the operation of a nuclear power reactor licensed pursuant to part 50 of this chapter, must include a cyber security plan that demonstrates how the applicant plans to meet the requirements of 10 CFR 73.53 of this chapter.

- Section 70.32(f) requires that the licensee make no change which would decrease the effectiveness of the cyber security plan prepared pursuant to 10 CFR 70.22(o) without the prior approval of the Commission. A licensee desiring to make such a change shall submit an application for an amendment to its license pursuant to 10 CFR 70.34. The licensee may make changes to the cyber security plan without prior Commission approval if these changes do not decrease the effectiveness of the plan. The licensee shall retain a copy of the cyber security plan and maintain records of changes to the plan made without prior Commission approval, for three years from the effective date of the change, and shall, within two months after the change is made, furnish a report containing a description of each change to the Director, Division of Security Policy, Office of Nuclear Security and Incident Response; the report may be sent using an appropriate method listed in 10 CFR 70.5(a), and a copy of the report must be sent to the appropriate NRC Regional Office shown in appendix A to part 73 of this chapter.

- Section 73.53 requires licensees to establish, implement, and maintain a cyber security program that will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern.

Related Guidance

RG 5.70, "Guidance for the Application of the Theft and Diversion Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.45 and 73.46" (not in the agency wide documents access and management system (ADAMS) and not publicly available because it contains classified information), further describes the adversary characteristics, tactics, techniques, and procedures to assist Category I FCF licensees to further develop their protective strategies against the design basis threat (DBT). RG 5.70 provides guidance on how site-specific security plans should consider the DBT but does not provide guidance on how to detect, protect against, or respond to a cyber attack.

Purpose of Regulatory Guides

The NRC issues RGs to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in

evaluating specific problems or postulated accidents, and to provide guidance to licensees. RGs are not substitutes for regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG contains and references information collections covered by 10 CFR Sections 40.31(n), 40.32(h), 70.22(o), 70.32(f), 73.53(a), 73.53(e), and 73.53(h) that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget (OMB), control numbers 3150-0020, 3150-0009 and 3150-0002.

Public Protection Notification

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

TABLE OF CONTENTS

B. DISCUSSION

Reason for Development

This new RG provides FCF licensees with an acceptable approach for meeting the requirements of 10 CFR 73.53. It also provides a methodology that licensees may use to establish, implement, and maintain a cyber security program that will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. In addition, it provides guidance on how to conduct an analysis to identify digital assets[1] associated with a consequence of concern and a process to determine which of those digital assets require protection from cyber attacks. Finally, this RG describes the elements required in a cyber security plan, includes a cyber security plan template (Appendix A), contains cyber security controls applicable to each type of consequence of concern (Appendices B – F), and provides an example implementing procedure (Appendix G).

Background

In recent years, the threat of cyber attacks has steadily risen, both globally and nationally. The U.S. Government has observed an increase in: 1) the number of cyber attacks; 2) the level of sophistication of such attacks; and 3) the potential for these attacks to impact numerous digital assets, including digital assets used at nuclear fuel cycle facilities. Additionally, these attacks can be conducted anonymously from remote locations throughout the world.

In response to the terrorist attacks of September 11, 2001, the NRC issued a series of security orders to prevent certain potential consequences from occurring due to a physical attack on FCF licensees. These orders addressed the threat environment at that time by imposing additional security requirements beyond those in 10 CFR 73.20, 73.40, 73.45, 73.46, and 73.67. The NRC also issued a separate security order to certain FCF licensees governing the protection of certain radiological and hazardous chemicals at their facilities. In addition to physical security requirements, the Interim Compensatory Measures Orders issued to FCF licensees in 2002 and 2003 contained a generic cyber security measure directing licensed facilities to evaluate and address cyber security vulnerabilities. This generic cyber security requirement did not specify or provide guidance for FCF licensees on: (1) detecting, protecting against, or responding to a cyber attack; or (2) establishing a formal cyber security program. Furthermore, the orders provided limited guidance on the implementation of cyber security for safety and security digital assets, focusing on computer systems that conduct and maintain communications during emergency response actions.

In 2007, the Commission promulgated a rulemaking entitled "Design Basis Threat" (72 *Federal Register* [FR] 12705) (Ref. 1), revising 10 CFR 73.1 to explicitly include a cyber attack as an element of the DBT. The DBT is used by certain licensees to form the basis for site-specific defensive strategies. RG 5.70, "Guidance for the Application of the Theft and Diversion Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.45 and 73.46" (not publicly available because it contains classified information), was developed to further describe the adversary characteristics, tactics, techniques, and procedures to assist Category I FCF licensees to further develop their protective strategies against the DBT. This RG provides guidance on how site-specific security plans should consider the DBT but does not provide FCF licensees guidance on detecting, protecting against, or responding to a cyber attack.

---

[1] For the purposes of this guidance, digital assets are defined as electronic devices or organized collections of devices that either process information, communicate data, or are programmed to manipulate licensee site machinery.

In March 2009, the NRC further addressed cyber security during publication of the Power Reactor Security Requirements final rule (74 FR 13926) (Ref. 2). The cyber security requirements for power reactors were placed into a stand-alone section in 10 CFR 73.54. The cyber security rule requires power reactor licensees to provide high assurance that digital computer and communication systems and networks associated with nuclear power reactor safety, security, and emergency preparedness functions are protected from cyber attacks. The development of associated guidance for implementing the requirements in 10 CFR 73.54 resulted in the publication of RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 3).

In June 2012, the NRC staff completed SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," (Ref. 4) which established the NRC staff's approach for evaluating the need for cyber security requirements for the following four categories of NRC licensees and facilities: 1) FCFs; 2) non-power reactors; 3) independent spent fuel storage installations; and 4) byproduct materials licensees. The roadmap reflects a graded approach to developing cyber security requirements commensurate with the inherent nuclear safety and security risks associated with the different types of licensees and facilities.

In 2014, the NRC staff issued SECY-14-0147, "Cyber Security for Fuel Cycle Facilities" (not publicly available because it contains security-related information, ADAMS Accession No.: ML14177A264). In SECY-14-0147, the NRC staff concluded that cyber security requirements for FCF licensees need to be addressed because of: 1) an increasing and persistent cyber security threat; 2) the potential exploitation of vulnerabilities through a variety of attack vectors; 3) the inherent difficulty of detecting the compromise of digital assets; and 4) the potential consequences associated with a cyber attack. In the Staff Requirements Memorandum to SECY-14-0147, the Commission directed the NRC staff to proceed directly with a cyber security rulemaking to apply a disciplined, graded approach to the identification of digital assets and a graded, consequence-based approach to their protection. This RG provides a comprehensive approach to meeting the cyber security requirements for systems within the scope of 10 CFR 73.53.

This RG provides guidance to assist in the identification of digital assets associated with each type of identified consequence of concern and a process for determining which digital assets must be protected from cyber attacks. Digital assets that must be protected are referred to as "vital digital assets" (VDAs). In accordance with 10 CFR 73.53(d)(5), FCF licensees must protect VDAs by taking measures to address the performance specifications of the cyber security controls specific to each of the applicable types of consequences of concern. FCF licensees may use the cyber security controls provided in the appendices to this RG or develop their own sets of cyber security controls. Cyber security controls must satisfy the stated regulatory requirements and should be based off industry accepted standards (e.g., National Institute of Standards and Technology (NIST), the joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC), Control Objectives for Information and Related Technologies, or International Society of Automation).

This RG offers a licensee guidance on addressing the necessary cyber security controls for an existing or new digital asset. This RG was informed by well-known and well-understood sets of cyber security controls from the NIST computer security standards. Taking measures to address the performance specifications of appropriate security controls satisfies elements of the cyber security program performance objectives as described in 10 CFR 73.53(b). This RG provides a flexible programmatic approach with which the licensee can successfully establish, maintain, and implement a cyber security program.

This RG provides guidance on the requirements of 10 CFR 73.53. The major sections of this RG are summarized below.

- Chapter C, Section 1, "General Requirements," provides an overview of the regulatory requirements relevant to cyber security.

- Chapter C, Section 2, "Cyber Security Program Performance Objectives," describes the purpose of the cyber security program. This section explains why the objectives are necessary for FCF licensees and how the objectives are achieved through implementation of the requirements in 10 CFR 73.53. Additional guidance is provided in Chapter C, Section 2 that describes the detection of a cyber attack capable of causing a consequence of concern. To meet the detection requirement in 10 CFR 73.53(b), the licensee should create a robust detection process that integrates into the management of the cyber security program.

- Chapter C, Section 3, "Cyber Security Team," describes the personnel which should be assigned by the licensee to develop the cyber security program to meet the requirements of 10 CFR 73.53(d)(1). The training and qualifications of the Cyber Security Team (CST) are also provided.

- Chapter C, Section 4, "Cyber Security Plan," describes the documentation licensees must develop to describe the cyber security program and submit to the NRC for review and approval. The cyber security plan references cyber security controls, specific to each type of consequence of concern, which the licensee must address to protect VDAs.

- Chapter C, Section 5, "Consequences of Concern," describes the minimum thresholds for each type of consequence of concern. A digital asset is vital if its compromise by a cyber attack would result in a consequence of concern. Consequences of concern that are directly caused by a cyber attack are "active" consequences of concern; consequences of concern that result from a secondary event that exploits the compromise of a digital asset are "latent" consequences of concern. The four types of consequences of concern are: 1) latent – design basis threat; 2) latent – safeguards; 3) active – safety; and 4) latent – safety and security. The consequences of concern and their minimum thresholds are defined in 10 CFR 73.53(c).

- Chapter C, Section 6, "Identification of Digital Assets and Support Systems," describes a methodology in which licensees:

    - Conduct an analysis to identify digital assets that are associated with a type of consequence of concern;
    - Evaluate each identified digital asset to determine if an alternate means (which is itself protected from cyber attack) is available to prevent the consequence of concern--if not, the digital asset is considered vital and requires cyber security controls; and
    - Conduct an additional analysis on each VDA to determine if it is associated with a support system that, if compromised by a cyber attack, could lead to a consequence of concern. If so, then the associated support system requires cyber security controls.

- Chapter C, Section 7, "Cyber Security Controls," describes the process of addressing the minimum cyber security controls needed to protect VDAs from cyber attacks that could result in a consequence of concern. Licensees are required by 10 CFR 73.53(e)(1) to identify the cyber security controls as part of their NRC-approved cyber security plan. Each cyber security control selected (or established by the licensee) must be documented for each VDA based on the type of consequence of concern.

- Chapter C, Section 8, "Implementing Procedures and Interim Compensatory Measures," describes the procedures and documentation that must be developed for each VDA. Guidance is provided on the type of information that should be included within the implementing procedures, its intended uses, and the need to maintain them for NRC inspections. This section also describes aspects of interim compensatory measures, including documenting a degraded cyber security control, tracking the interim compensatory measure to completion, and restoring and testing the cyber security control.

- Chapter C, Section 9, "Configuration Management," describes cyber security configuration management and some of the site-wide elements that should be considered.

- Chapter C, Section 10, "Review of the Cyber Security Program," describes the requirements for the periodic review of the cyber security program. This review serves to evaluate the overall effectiveness and adequacy of the cyber security program.

- Chapter C, Section 11, "Event Reporting and Tracking," describes the event reporting and tracking requirements of 10 CFR 73.53(h).

- Chapter C, Section 12, "Recordkeeping," describes the retention of all records and supporting technical documentation required to satisfy the requirements of the regulation until the Commission terminates the license for which the records were developed.

- Appendix A, "Cyber Security Plan Template," contains a template demonstrating an example of acceptable format and content for the cyber security plan, required to be submitted to the NRC in accordance with 10 CFR 73.53(a). The template can be used by FCF licensees to assist with documenting compliance with the regulatory requirements and to assist the NRC staff with the review process.

- Appendices B, C, D, E, and F contain cyber security controls, specific to each type of consequence of concern, acceptable to the NRC staff for establishing the performance specifications for which measures will be taken to protect VDAs. A licensee may use these cyber security controls or develop their own, ideally based on another standard, as long as the regulatory requirements of 10 CFR 73.53 are met.

- Appendix G contains an example of an implementing procedure. The simplified example can be used by FCF licensees to assist with developing site-specific implementing procedures for VDAs.

The requirements of 10 CFR 73.53(a) and the template provided in Appendix A of this document outline timeframes for completing specific milestones associated with this rulemaking. These timeframes are summarized below, in Table B-1.

TABLE B-1

Milestone	Timeframe
Licensee submits the cyber security plan, through an application for amendment of its license, to the NRC for review	Within 180 days of publication of the final rule
The NRC reviews and approves the license amendment request and cyber security plan	Typically within 150 days of submission
Licensee conducts analyses to identify and document each digital asset associated with a consequence of concern and determines: (1) VDAs and (2) digital assets with an acceptable alternate means	Within 6 months of NRC approval of the cyber security plan.
Full implementation of the NRC approved cyber security plan	Within 18 months of NRC approval of the cyber security plan.

Harmonization with International Standards

The International Atomic Energy Agency (IAEA) established a series of security guides, standards, and technical reports addressing concepts and considerations for achieving a high level of security for protecting people and the environment. IAEA security guides present international good practices and increasingly reflect best practices to help users striving to achieve high levels of security. Pertinent to this RG, IAEA Nuclear Security Series No.: 17, "Computer Security at Nuclear Facilities," issued in December 2011 (Ref. 5), addresses concepts and considerations for cyber security at nuclear facilities. IAEA Nuclear Security Series No.: 23-G, "Implementing Guide for Security of Nuclear Information," issued February 2015 (Ref. 6), addresses steps required to effectively execute an information security plan including cyber security issues. More specifically, the IAEA Nuclear Energy Series Technical Report NP-T-1.13, "Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants," issued November 2015 (Ref. 7), discusses the challenges of addressing cyber security protections in the context of implementing and maintaining digital instrumentation and control. While these documents do discuss cyber security at length, they are primarily designed for use with nuclear power reactors rather than FCF licensees. As such, this RG incorporates similar general concepts and is consistent with the basic cyber security principles provided in IAEA Security Series Nos.: 17 and 23-G, and Nuclear Energy Series Technical Report NP-T-1.13.

The NRC staff also reviewed guidance from ISO/IEC and identified the ISO/IEC 27000 series "Information Security Management System (ISMS), Family of Standards" (Ref. 8) This family of standards, revised in 2016, is designed to provide comprehensive guidance and controls for cyber security and the management of information security. ISO/IEC 15408, "The Common Criteria for Information Technology Security Evaluation," revised in 2012 (Ref. 9), is an international standard for cyber security certification for information technology products. Because both standards are designed for organizations and vendors of varying sizes and disciplines they are deliberately broad in scope and not specifically related to the nuclear fuel cycle industry. As a result, this RG incorporates related basic guidance and provides mapping to specific controls and other informative references where appropriate.

Documents Discussed in Staff Regulatory Guidance

This RG draws information, in part, from one or more standards and guidance documents developed by the NIST. These standards and guidance documents contain information on the cyber security risk management framework and cyber security controls that a licensee may wish to reference for additional information.

C. STAFF REGULATORY GUIDANCE

1 General Requirements

The regulations in 10 CFR 73.53 identify the requirements needed to meet the cyber security program performance objectives for FCF licensees. The cyber security program performance objectives are identified in 10 CFR 73.53(b), which requires a licensee to establish, implement, and maintain a cyber security program that will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The rule identifies four types of consequences of concern that establish thresholds for potential events involving radiological and chemical exposures, classified information or matter, special nuclear material (SNM) of moderate strategic significance, and a formula quantity of strategic SNM. These events must be prevented to protect public health and safety and promote the common defense and security. The cyber security program consists of: 1) establishing and maintaining a CST; 2) developing a site-specific cyber security plan which is submitted to the NRC for review and approval; 3) conducting an analysis to identify digital assets associated with a consequence of concern and evaluating the digital assets to determine if they require protection (i.e., if they are VDAs); 4) establishing and maintaining written implementing procedures for VDAs and documenting the measures taken to address the performance specifications associated with the identified cyber security controls; 5) providing interim compensatory measures to meet the cyber security program performance objectives when the cyber security controls are degraded ; and 6) managing the cyber security program to detect, protect against, and respond to cyber attacks capable of causing a consequence of concern.

1.1 Cyber Security Team

In accordance with 10 CFR 73.53(d)(1), licensees must establish and maintain an adequately structured CST consisting of competently trained and qualified staff. The team should include members who have expertise in cyber security and draw upon staff with safety, security, and safeguards knowledge. The team must have the appropriate resources available to be effective. The team is responsible for implementing a cyber security program that meets the requirements of 10 CFR 73.53. Additional guidance on the CST is provided in Chapter C, Section 3 of this document.

1.2 Cyber security plan

In accordance with 10 CFR 73.53(e), licensees must establish, implement, and maintain a site-specific cyber security plan. Current licensees are required by 10 CFR 73.53(a) to submit, through an application for amendment of their license, a cyber security plan for NRC review and approval. Future applicants are required by 10 CFR 40.31(n) or 70.22(o), as appropriate, to submit a cyber security plan for NRC review and approval as part of their license application. The cyber security plan should describe the facility's cyber security program with sufficient detail for the NRC to determine compliance with the regulations in 10 CFR 73.53. To meet the requirements of 10 CFR 73.53(e)(1), the cyber security plan must, at a minimum: 1) document that the CST is adequately structured, staffed, trained, qualified, and equipped to manage the cyber security program and 2) specify the cyber security controls that the licensee will address to protect VDAs from cyber attacks and prevent consequences of concern. Also, in accordance with 10 CFR 73.53(e)(2), the cyber security plan must describe the licensee's measures for: 1) management and performance of the cyber security program; and 2) incident response (IR) to a cyber attack affecting VDAs. Upon implementation of the licensee's approved cyber security plan, the cyber security program will be routinely inspected by the NRC for compliance with 10 CFR 73.53. Additional guidance on the cyber security plan is provided in Chapter C, Section 4 of this document. Appendix A of this document, contains a template demonstrating an example of acceptable format and content for the cyber security plan, required to be submitted to the NRC in accordance with 10 CFR 73.53(a).

1.3 Identifying digital assets

In accordance with 10 CFR 73.53(d)(3) and (4), licensees must identify digital assets associated with a type of consequence of concern and further evaluate whether an alternate means (protected from a cyber attack) is available that will prevent the consequence of concern in the event that a cyber attack compromises the digital asset. Additional guidance on the identification of digital assets is provided in Chapter C, Section 6 of this document.

In accordance with 10 CFR 73.53(d)(4), licensees must determine which of the identified digital assets are vital. A digital asset is not considered vital if an alternate means is available to prevent the consequence of concern and that alternate means cannot be compromised by a cyber attack. Only VDAs are required to be protected against a cyber attack by 10 CFR 73.53(d)(5). As part of this analysis, licensees will also identify associated support systems for VDAs that, if compromised by a cyber attack, could lead to a consequence of concern. The term VDA is inclusive of all components necessary to perform the function needed to prevent the consequence of concern. Additional guidance on the identification of VDAs is provided in Chapter C, Section 6 of this document.

1.4 Addressing performance specifications of cyber security controls

In accordance with 10 CFR 73.53(d)(2) and (d)(5), licensees must take measures, for each VDA, to address the performance specifications of the applicable cyber security controls based on the type of consequence of concern. Licensees may elect to group similar types of VDAs together. This gives licensees the opportunity to develop a common control, or sets of common controls, for multiple VDAs. The licensee is responsible for addressing the appropriate controls and related parameters to ensure that the consequence of concern associated with a VDA will be prevented. Additional guidance on cyber security controls is provided in Chapter C, Section 7 of this document. Appendices B, C, D, E, and F of this document contain cyber security controls that the NRC staff finds acceptable for protecting VDAs specific to each of the four types of consequence of concern. A licensee may use these cyber security controls or develop their own using a recognized standard as long as the regulatory requirements of 10 CFR 73.53 are met.

1.5 Implementing procedures and interim compensatory measures

In accordance with 10 CFR 73.53(5)(ii) the licensee must establish and maintain written implementing procedures for VDAs, documenting the measures taken to address the performance specifications associated with the identified cyber security controls. Acceptable implementing procedures document the cyber security controls, based on the type of consequence of concern. Note that similar VDAs with common controls may also have implementing procedures in common. Additional guidance on implementing procedures is provided in Chapter C, Section 8 of this document.

In accordance with 10 CFR 73.53(d)(6), the licensee is required to apply interim compensatory measures when the measures taken to address the performance specifications associated with the identified cyber security controls are degraded. When implemented, interim compensatory measures must be documented, tracked to completion, and available for inspection by the NRC staff. These interim compensatory measures may be captured in the implementing procedures, or they could be part of other site-specific documentation. Additional guidance on interim compensatory measures is provided in Chapter C, Section 8 of this document.

1.6 Managing the cyber security program

A licensee's cyber security plan is required by 10 CFR 73.53(e)(1) to describe how the licensee will satisfy the regulatory requirements and manage the cyber security program. The cyber security program performance objectives in 10 CFR 73.53(b) establish critical program elements that address the evolving cyber security threat, which is likely to become more prevalent and sophisticated over time. As such, the means for management of the cyber security program are needed to maintain its effectiveness and adequacy. The requirements in 10 CFR 73.53(f) through (i) are: configuration management; review of the cyber security program; event reporting and tracking; and recordkeeping. The requirements in 10 CFR 73.53(f) through (i) establish the means for management of cyber security program over the life of the facility. These elements of the cyber security program should be incorporated and conducted as part of the licensee's standard operations. Additional guidance is provided on: configuration management in Chapter C, Section 9; review of the cyber security program in Chapter C, Section 10; event reporting and tracking in Chapter C, Section 11; and recordkeeping in Chapter C, Section 12 of this document.

2 Cyber Security Program Performance Objectives

In accordance with 10 CFR 73.53(b), a licensee must establish, implement, and maintain a cyber security program that will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The cyber security requirements set forth in 10 CFR 73.53 are intended to be performance based to allow licensees flexibility with implementation while protecting public health and safety and promoting common defense and security. The performance objectives to detect, protect against, and respond to cyber attacks are critical program elements for addressing the evolving cyber security threat, which is likely to become more prevalent and sophisticated over time.

2.1 Detect a cyber attack capable of causing a consequence of concern

As required by 10 CFR 73.53(b), the licensee must implement a cyber security program that will detect a cyber attack capable of causing a consequence of concern. To meet this requirement, the licensee should develop a robust detection process consistent with the controls located in the Appendices. The detection process should include data collection points and analysis mechanisms, where technically feasible. This process should have the necessary equipment, materials, procedures, and sensors for the licensee to analyze anomalous activity.

Application of the controls provides an acceptable approach for implementing the detection process to identify when a VDA is subject to a cyber attack. The licensee should maintain a baseline understanding of the facility's normal data communications and network system behavior related to VDAs. This provides a frame of reference which is useful to support the identification of unusual activity or communications. The licensee should maintain awareness of the characteristics of cyber attacks through appropriate training, monitoring relevant threat intelligence resources, and lessons learned to improve early recognition of cyber attacks.

Licensees should use lessons learned from the detection of new cyber security threats or attacks to inform and update, where applicable, their cyber security program. An acceptable detection process allows identification of abnormal activity on VDAs in a timely manner so the licensee can respond, evaluate the potential impacts, and take compensatory measures, if needed. Detection also provides the CST information on the type of attacks occurring against the facility so the licensee can maintain adequate protective measures and response capabilities. Compliance with the detection objective provides awareness of the ongoing cyber security threat and supports understanding of the effectiveness of the cyber security program.

The licensee should utilize relevant threat intelligence sources to inform the detection process (e.g., Government agencies, private cyber security organizations, or private industry data). Licensees should review the resulting data from the cyber security detection process and relevant threat information, at a minimum, on a quarterly basis. Useful information should be communicated to the appropriate internal organizations to support maintaining adequate protection for the VDAs. The detection process should be reviewed consistent with 73.53(g) to confirm its proper function. Analysis efforts should be reviewed for accuracy. Overall, the licensee should seek to continuously improve its detection processes and efforts.

2.2 Protect against a cyber attack capable of causing a consequence of concern

As required by 10 CFR 73.53(b), the licensee must protect against a cyber attack capable of causing a consequence of concern. This performance objective is necessary to maintain safety, security, and safeguards at a FCF licensee. FCF licensees rely on digital assets to perform safety, security, and safeguards functions. Unprotected VDAs could be compromised by a cyber attack and either: 1) cause a consequence of concern (i.e., active); or 2) cause the digital asset to not perform its intended function when called upon (i.e., latent consequence of concern). Cyber attacks may have various attack vectors (e.g., wired, wireless, hand carried) to exploit unprotected VDAs. In addition, cyber attacks can be launched remotely, occur over a broad timeframe, and compromise multiple digital assets simultaneously with an immediate or delayed impact (i.e., an active or latent consequence of concern). Analysis of digital assets associated with a consequence of concern is needed to determine which safety, security, and safeguards digital assets, if any, require protection against cyber attacks.

Licensees are expected to ensure that appropriate cyber security controls are maintained to protect the associated VDAs, in accordance with 10 CFR 73.53(d)(5). Licensees are also expected to use proper configuration and change management techniques when making alterations or updates to VDAs, in accordance with 10 CFR 73.53(f). All licensees should assess plant changes to determine if cyber security associated with a consequence of concern is affected and if additional protection efforts are needed. This activity forms the basis of the protection objective and should be conducted throughout the life cycle of the facility. When properly implemented in compliance with requirements in 10 CFR 73.53, configuration management supports assurance of protection against a cyber attack capable of causing consequence of concern.

Additional guidance regarding the cyber security protection required by 10 CFR 73.53 is provided by this document in Chapter C: Section 3 for the CST; Section 4 for the cyber security plan; Section 5 for consequences of concern; Section 6 for identification of digital assets; Section 7 for cyber security controls; Section 8 for implementing procedures and interim compensatory measures; Section 9 for configuration management; Section 10 for the review of the program; Section 11 for event reporting and tracking; and Section 12 for recordkeeping.

2.3 Respond to a cyber attack capable of causing a consequence of concern

As required by 10 CFR 73.53(b), the licensee must respond to a cyber attack capable of causing a consequence of concern. While the cyber security program is designed to protect against cyber attacks, impenetrable cyber security is not achievable. Therefore, effective and timely response to cyber attacks is important to minimize potential impacts. Given the nature of the cyber threat, licensees should establish procedures and resources for response to cyber attacks that may exploit a VDA.

The response effort by the licensee to an attack on a VDA should be to first place the digital asset into a safe condition and eliminate the potential for a consequence of concern. Once the potential compromise is prevented, the next effort should be to stop the attack. This removes the threat of cyber

attack toward other VDAs and allows for eradication of potential malware. Finally, the licensee should preserve, where possible, all evidence of the attack for investigation. Additional guidance on recordkeeping is provided in Chapter C, Section 12 of this document.

When a cyber attack is detected, the CST should confer with the physical security and safety programs to ensure appropriate coordination. If a cyber security response cannot stop the cyber attack, from causing a consequence of concern, the CST should defer to the appropriate program that would address the consequence.

The ability of the licensee's cyber security program to respond to a cyber attack should be tested regularly, where technically feasible. Licensees should take protective measure to prevent testing from introducing vulnerabilities. This can be prevented by testing systems prior to installation, conducting table top exercises on critical systems, or evaluating software in "sand-box" (i.e., isolated) conditions. When issues are identified through testing, they should be incorporated into the facility's corrective actions, and, if appropriate, be used to inform the facility's protective strategies and detection methods. Overall, these response exercises should improve the licensee's ability to effectively respond to a cyber attack. Guidance on the CST's involvement with responding to a cyber attack is provided in Chapter C, Section 3 of this document.

After a licensee responds to a cyber attack and the resulting impacts of that attack, 10 CFR 73.53(h) has specific event reporting and tracking requirements. Guidance on event reporting and tracking is provided in Chapter C, Section 11 of this document.

3 Cyber Security Team

As required by 10 CFR 73.53(d)(1), the licensee must establish and maintain a CST that is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program. The CST is responsible for ensuring compliance with the performance objectives of 10 CFR 73.53 through the implementation of the cyber security program. The specific responsibilities of the CST are to: establish and maintain cyber security controls capable of preventing a cyber attack from causing a consequence of concern, identify digital assets that if compromised could result in a consequence of concern, and determine which digital assets are vital. To accomplish this, the CST should ensure the facility:

- Protects VDAs and associated support systems from cyber attacks capable of causing a consequence of concern;
- Configures, operates, and maintains cyber security equipment to both detect and protect against a cyber attack capable of causing a consequence of concern;
- Understands the cyber security aspects of the facility network architecture, hardware platforms, software platforms, operating systems, process-specific applications of digital assets, and the services and protocols upon which those applications rely;
- Performs cyber security evaluations of digital assets, determines alternate means of protection, and takes measures to address the performance specifications of the appropriate cyber security controls;
- Conducts security audits, vulnerability assessments, network scans, table top simulations, or penetration tests against VDAs, where technically feasible without compromising the system;

- Authorizes VDAs for use by the licensee, assign individuals to fulfill specific roles and responsibilities for this authorization process;
- Manages, documents, and reports the security state of VDAs;
- Assesses cyber threat intelligence and new vulnerability information;
- Conducts cyber security investigations following the compromise of VDAs;
- Preserves forensic evidence collected during cyber security investigations to prevent loss of evidentiary value;
- Created a trained and qualified cyber security workforce through ongoing professional development;
- Maintains appropriate skill and knowledge in the area of cyber security;
- Perform duties with independence from the facility's operations, using well-defined responsibilities and sufficient authority to carry out those responsibilities;
- Perform, in part, as a cyber security incident response team (CSIRT);
- Provides role-related cyber security training and awareness to licensee staff members associated with VDAs; and
- Supports the cyber security configuration management system consistent with 10 CFR 73.53(f).

The CST is a permanent organizational unit within the licensee's facility. While team members can have responsibilities outside those of the CST, these responsibilities should not interfere with the individual's cyber security duties. The team can also include corporate or contract personnel provided these individuals are appropriately qualified for the role and authorized for a position on the team.

The CST should be the licensee's internal resource for cyber security threat information. It should also coordinate cross-organization cyber security threat information-sharing with the physical security and emergency preparedness programs. The team is responsible for maintaining the cyber security program by keeping the cyber security practices, techniques, and technologies up to date.

3.1 Structure and staffing

The CST should consist of individuals that include management, cyber security experts, and technical experts with knowledge of the facility's safety, security, and safeguards functions. A licensee can form a CST by defining and documenting roles, responsibilities, authorities, and functional relationships. These roles should be clearly communicated to the appropriate site organizations and individuals (e.g., employees, subcontractors, temporary employees, visiting researchers, and vendor representatives). A group of personnel administering the cyber security program that the NRC would find acceptable includes the following four categories of individuals:

- A cyber security program sponsor who is a member of senior site management (executive level) and provides oversight and accountability for the cyber security program. The senior manager

provides oversight for the cyber security program that is independent from operations and has adequate resources and stop work authority.

- A cyber security program manager who is responsible for coordinating, developing, implementing, and maintaining the cyber security program. This individual provides oversight and direction to the CST. The individual serves as the single point of contact between upper management and the CST, responsible for implementing the commitments in the cyber security plan.

- Cyber security specialists who are responsible for implementing the cyber security program. These individuals conduct the day-to-day operations of the cyber security program. They are responsible for providing technical expertise to the operational staff for implementation of the cyber security program. They ensure digital assets are protected consistent with the cyber security plan and monitor digital assets for indicators of a cyber attack. They keep knowledgeable of the evolving threat environment. These individuals maintain the cyber security program over time.

- Technical staff from facility organizations including security, operations, engineering, emergency preparedness, and other support organizations, as required, who are responsible for maintaining alternate means to address digital assets associated with a consequence of concern as well as implementing controls for protection of VDAs. These members may or may not be part of the CST, but they provide technical input on the analysis of digital assets.

The team's organizational structure should be summarized in the cyber security plan consistent with the requirements of 10 CFR 73.53(i).

3.2 Training and qualification

The licensee must ensure that the CST members are appropriately trained and qualified to effectively implement and maintain the cyber security program.

Training

The CST is responsible for developing and maintaining the facility's cyber security training. The CST is responsible for determining the appropriate level of basic cyber security awareness training commensurate with an each individual's assigned roles and responsibilities. The training requirements and records can be maintained as part of the facility's overall training program.

A minimum level of training should also be provided for each position on the CST depending on the roles and responsibilities of that position. Training for the CST should be identified in the cyber security plan. In addition, the actual training should be documented in procedures. The licensee should keep records to indicate that training is up-to-date. Additional training requirements may be necessary to ensure familiarity with the controls applied to VDAs.

Qualification

The license should establish and document minimum qualification requirements for each key position on the CST. The individual's qualifications should be documented and available for review. The cyber security program sponsor should have experience in working with digital assets or network systems. The cyber security program manager should have an industry recognized certification in a cyber security related field (e.g., Certified Information Systems Security Professional) and experience working

in the cyber security field. The cyber security specialists should have experience in networking, systems administration, database management, vulnerability scanning, penetration testing, or web applications. The technical staff that support the CST should have a working knowledge of the digital assets used throughout their area of operations. These individuals should not assume their assigned positions until they are properly trained and qualified to perform their responsibilities.

3.3 Equipment

The CST should be appropriately provided with the necessary software, tools, and devices to analyze networks and related traffic, scan devices to verify digital assets are operating within acceptable parameters and support the periodic audit of the VDA defenses. This equipment should be routinely updated or replaced to reflect the current operating environment as well as the latest information from common vulnerabilities and exposures compatible databases (e.g., National Cyber Security federally funded research and development center, the U.S. Department of Homeland Security Industrial Control Systems, U.S. Department of Homeland Security Cyber Emergency Response Team).

4 Cyber Security Plan

As required by 10 CFR 73.53(e), licensees must establish, implement, and maintain a site-specific cyber security plan that describes how the licensee will satisfy the requirements of the regulation. The cyber security plan should provide an overview of the policies and procedures that support the development and implementation of the cyber security plan, as well as the management commitment to this effort. In accordance with 10 CFR 73.53(e)(1), the cyber security plan documents the cyber security controls that will be used to protect against cyber attacks capable of causing the consequences of concern. Under 10 CFR 73.53(a), the cyber security plan is incorporated into the NRC license as a license condition. The plan describes the licensee's cyber security program and how the program complies with the requirements in 10 CFR 73.53. The plan should addresses technical (e.g., network infrastructure), physical (e.g., digital assets used at the facility), and personnel (e.g., staff training and responsibilities) components of the program. The cyber security plan should demonstrate the licensee's commitment to maintain cyber security policies and procedures up to date and applicable among organization entities.

Licensees should include in their cyber security plan their goals for addressing cyber security in their daily operations for protection of VDAs. Licensees should also describe how cyber security is integrated into the design architecture of their site. At each step of the cyber security plan's development, site-specific considerations should be addressed to ensure the resulting document accurately depicts the commitments and conditions specific to the licensee.

The cyber security plan should describe or reference the written policies and procedures maintained on site for the implementation of the cyber security program. In addition, the cyber security plan should describe how the licensee will identify, evaluate, and protect against emergent cyber security threats that develop over time. The cyber security plan should reference the procedures for maintaining this analysis capability throughout the life of the facility.

4.1 Elements of a cyber security plan

To further guide licensees, Appendix A to this RG provides a generic cyber security plan template that can be used to develop a cyber security plan and to establish and maintain a cyber security program that will comply with the requirements of 10 CFR 73.53.

A cyber security plan describes the means and governing procedures to ensure that cyber security information, associated records, and implementing policies and procedures are appropriately evaluated,

consistent with applicable requirements in 10 CFR 73.21 and 73.22 for protection of safeguards information, and the requirements of 10 CFR Part 95 for protection of classified information. Revisions to the cyber security plan must be processed in accordance with 10 CFR 40.32(h) or 10 CFR 70.32(f), whichever is applicable to the specific FCF licensee. A licensee must submit changes that would result in a decrease in the effectiveness of the cyber security plan, to the NRC for review and approval prior to implementation.

As required by 10 CFR 73.53(e), the cyber security plan must describe how the licensee will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern identified in 10 CFR 73.53(c). The cyber security plan must address the following elements:

- Documentation that the CST is established and maintained in accordance with 10 CFR 73.53(d)(1). This would include sufficient detail to demonstrate the CST is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program as required by 10 CFR 73.53(d)(1).

- Description of the cyber security controls and associated performance specifications for which measures will be taken to prevent a cyber attack from causing a consequence of concern, as required in 10 CFR 73.53(d)(2).

- Description of the identification process for digital assets associated with applicable consequences of concern, as required in 10 CFR 73.53(d)(3).

- Description of the identification process for alternate means, VDAs, and associated support systems as required in 10 CFR 73.53(d)(4).

- Description of the process to take measures to address the performance specifications of the identified cyber security controls for VDAs to assure protection against a cyber attack capable of causing a consequence of concern, as required by 10 CFR 73.53(d)(5). This should include describing the process for:
    - Determining the measures (e.g., physical hardware, software, activities) to be used to meet the parameters of the selected cyber security controls;
    - Justifying not taking measures to address the performance specifications of controls that are not applicable to certain VDAs and documenting how equivalent protection is achieved; and
    - Establishing and maintaining written implementing procedures for these measures and justifications. Note that these implementing procedures are maintained outside of the cyber security plan.

- Description of how interim compensatory measures are applied, documented, and tracked to completion when the measures taken to address the performance specifications associated with the identified cyber security controls are degraded in order to meet the cyber security program performance objectives (10 CFR 73.53(d)(6)).

- Description of the configuration management system to be used to address facility changes for cyber security impacts as required by 10 CFR 73.53(f). This would include sufficient detail to demonstrate that these changes are evaluated prior to implementation and do not decrease the effectiveness of the cyber security program or affect its ability to meet the performance objectives listed in 10 CFR 73.53(b).

- Description of the periodic review process to be used to evaluate the cyber security program as required by 10 CFR 73.53 (g). This would include sufficient detail to demonstrate how the licensee will evaluate the effectiveness and adequacy of the program, controls, alternate means used, defensive architecture for digital assets, and the related implementing procedures. This would also include sufficient detail to demonstrate how the results will be addressed, tracked, and reported as required.

- Description of measures for cyber security incident response (CSIR) to a cyber attack affecting VDAs or that may cause a consequence of concern. In part, these requirements include event reporting and tracking as required by 10 CFR 73.53(h).

- Description of how a fully implemented cyber security program will be maintained and managed as required by 10 CFR 73.53(b) and 10 CFR 73.53(e)(1)(ii), respectively.

- Summary descriptions regarding cyber detection activities planned for use by the licensee.

- Confirmation that the licensee will meet the reporting requirements in 10 CFR 73.53(h). This affirmation should reference the log to be used for recordable events in accordance with 10 CFR 73.53(h)(2).

- Confirmation that the licensee will meet the recordkeeping requirements in 10 CFR 73.53(i). This affirmation should include the title for the position managing the records for records associated with 10 CFR 73.53 and the cyber security program.

Consistent with 10 CFR 73.53(e)(2), policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee to support the development and implementation of the cyber security plan need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by the NRC staff.

The cyber security plan itself is subject to the review requirement in 10 CFR 73.53(g) and should be updated, as needed. It should also be updated due to applicable changes in VDAs as part of overall configuration management system, as required by 10 CFR 73.53(f). Updates that would result in a decrease in the effectiveness of the cyber security plan will require NRC review and approval consistent with 10 CFR 40.32(h) or 10 CFR 70.32(f), whichever is applicable to the specific FCF licensee, prior to implementation of the change.

4.2 Managing the cyber security program

In accordance with 10 CFR 73.53(e)(1)(ii), a licensee's cyber security plan is required to describe how the cyber security program will be managed. This description should include the goals for operation after the program is fully implemented. The plan should also state how the CST and its functions will continue to support the cyber security program for the life of the facility, as described below.

Once the program is fully implemented, the licensee is required under 10 CFR 73.53(b) to maintain the cyber security program. The licensee should maintain the program through effective management of personnel, resources, and established activities. This management should start with the continued oversight and development by the CST of the cyber security program. This should also include the completion and supervision of the regular or periodic duties and activities to meet the performance objectives of as well as the specific performance specifications for cyber security controls associated with VDAs.

It is expected that the management of the fully implemented cyber security program would reflect the following concepts:

- Adaptive processes – The licensee adapts its cyber security practices based on lessons learned and predictive indicators derived from previous and current activities. Through a process of continuous improvement incorporating appropriate leadership, cyber security technologies and practices, the licensee should actively adjust to a changing cyber security landscape and respond to evolving and sophisticated threats in a timely manner.

- Integrated administration – The licensee implements an organization-wide approach to managing the cyber security program that uses risk-informed policies, processes, and procedures to address issues. Proper administration of the cyber security program is part of the organizational culture and evolves from the results of previous activities, information shared by other sources, and continuous awareness of activities associated with VDAs and the threats to their cyber security.

Licensees are expected to adjust management practices as necessary in order to maintain the effectiveness of the cyber security program. This would include making changes to reflect the recommendations stemming from the periodic review required by 10 CFR 73.53(g) and should incorporate lessons learned from the CSIR capability.

4.3 Cyber security incident response

A licensee's cyber security plan must describe the measures to respond to a cyber attack capable of causing a consequence of concern, consistent with 10 CFR 73.53(e)(2)(iii). This information must be documented in the cyber security plan or may be incorporated by referencing a cyber security incident response plan (CSIRP). The CSIRP should be distinct from a licensee's emergency plan and be maintained up to date. The CSIRP should document the roles, responsibilities, management commitment, and coordination among physical security and operations staff necessary to respond to cyber attacks. The cyber security plan should reference the CSIRP and commit to appropriate training on CSIR for applicable personnel. The CSIRP should be available for inspection by the NRC.

In accordance with 10 CFR 73.53(b), a licensee is required to respond to a cyber attack capable of causing a consequence of concern. To satisfy this requirement, licensees should form a CSIRT that includes members of the CST. The CSIRT should assess and provide a response to cyber attacks associated with a consequence of concern. The CSIRT staff should have experience in or access to digital forensics, malicious code analysis, tool development, and facility engineering. The CSIRT should be allocated sufficient resources to accomplish their role. Members of the CSIRT should receive role-specific CSIR training. Note that the CSIRT generally operates independent of the emergency plan but should support event response, as needed.

The CSIR should include cyber security capabilities that avert the consequence of concern and lead to safe shutdown of the VDA, as appropriate. The CSIR should complete detection and analysis, containment, eradication of malware and other related cyber intrusions, where feasible. The analysis should determine the extent and impact of a cyber attack and if compensatory measures need to be implemented. Mitigation strategies should be available for CSIR to prevent expansion of a cyber attack, limit its effects, and remove the threat. The CSIR activities should be coordinated with existing physical security and emergency preparedness.

For a cyber attack capable of causing a consequence of concern, the CSIR should have potentially affected VDAs enter a safe mode of operation or shutdown, where technically feasible. The licensee

should ensure that, during the CSIR, the capacity for information processing, telecommunications, and environmental support exists. The licensee should plan to maintain essential safety and security functions with no loss of continuity during a CSIR. Once the consequence of concern has been averted, the CSIRT should communicate with internal and external stakeholders to alert plant staff to monitor their systems for subsequent compromise. The licensee should consider engaging law enforcement to investigate the attacks when feasible and informing industry to be knowledgeable of the threat.

After a CSIR, the license must comply with the specific event reporting and tracking requirements set forth in 10 CFR 73.53(h). Guidance on event reporting and tracking is provided in Chapter C, Section 11 of this document. Licensees should also incorporate lessons learned into CSIR procedures, training, and testing. These lessons learned may also require changes to the CSIR plan. Compliance with the response performance objective serves to mitigate the effects of a cyber attack and supports improvement of the cyber security program.

The licensee should test the CSIR capabilities on a regular basis in conjunction with other security response or emergency preparedness drills. The licensee should conduct an exercise to simulate a cyber security event and allow for CSIR testing and training at least once during each periodic review cycle consistent with 73.53(g). The exercise itself should be as realistic as practicable in order to most effectively evaluate the capabilities of the cyber security program. The results of the exercises should be integrated into the training materials through regular updates as well as the overall CSIRP and related procedures.

4.4 Emergency plan

FCF licensees are required to address the emergency plan requirements consistent with 10 CFR 40.31(j) or 70.22(i). This should not be confused with development of the CSIRP which is an independent process for responding to cyber security attacks that have not yet caused a consequence of concern. If a cyber security response cannot prevent the cyber attack from causing a consequence of concern, the CSIRT should defer to the appropriate emergency plan response that would address the consequence. Once a cyber security incident rises to the level that the emergency plan is activated, the emergency plan would be used to respond to the event, even if it involved a cyber attack. The CSIRT should be used to respond to cyber attacks that do not involve, or have not yet involved, the emergency plan. The CSIRT may also be a resource utilized when implementing the emergency plan, if needed, but in these cases it should be made clear that the CSIRT would be operating off emergency plan procedures – not the CSIRP.

5 Consequences of Concern

In accordance with 10 CFR 73.53(c), a licensee's cyber security program must be designed to protect against the specified consequences of concern that are appropriate to the facility type of the licensee. The regulatory thresholds for consequences of concern at FCF licensees have been compiled in Table C-1, "Consequence of Concern and Related References," of this section. The consequence of concern thresholds were informed by the safety regulations in Part 70, security requirements in Parts 73 and 95, and material control and accounting requirements in Part 74, as specified in Table C-1.

The NRC is seeking to protect licensed activities that have the potential for a cyber attack to cause or result in radiological or chemical exposure or release; the loss or unauthorized disclosure of classified information or matter; the theft, diversion, or the loss of material control and accounting of nuclear material of moderate strategic significance; radiological sabotage, as specified in 10 CFR 73.1(a)(1); or the theft, diversion, or the loss of material control and accounting of a formula quantity of strategic special nuclear material. By targeting these consequences, the NRC intends for a licensee to

focus their cyber security efforts to effectively protect against cyber threats associated with risk-significant impacts.

TABLE C-1 – CONSEQUENCE OF CONCERN AND RELATED REFERENCES

SECTION 1 LATENT – DESIGN BASIS THREAT The compromise, as a result of a cyber attack at a licensee authorized to possess or use a formula quantity of strategic special nuclear material, of a function needed to prevent one or more of the following:	
• Radiological sabotage;	Reference 10 CFR 73.1(a)(1)
• Theft or diversion of formula quantities of strategic special nuclear material; or • Loss of nuclear material control and accounting for strategic special nuclear material.	References 10 CFR 73.1(a)(2) 10 CFR 73.20 10 CFR 74.51
SECTION 2 LATENT – SAFEGUARDS The compromise, as a result of a cyber attack at a licensee authorized to possess or use special nuclear material of moderate strategic significance, of a function needed to prevent one or more of the following:	
• Unauthorized removal of special nuclear material of moderate strategic significance; or • Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance.	References 10 CFR 73.67 10 CFR 74.41
SECTION 3 ACTIVE – SAFETY One or more of the following that directly results from a cyber attack:	
• Radiological exposure of 25 rem or greater for any individual; • 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or • An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.	References 10 CFR 70.61 10 CFR 70.62 10 CFR 40.31 and 10 CFR 70.22
SECTION 4 LATENT – SAFETY AND SECURITY The compromise, as a result of a cyber attack, of a function needed to prevent:	
• Radiological exposure of 25 rem or greater for any individual; • 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; • An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual; or	References 10 CFR 40.31 and 10 CFR 70.22
• Loss or unauthorized disclosure of classified information or classified matter.	Reference 10 CFR Part 95

The NRC has identified and developed four types of consequences of concern that are within the scope of 10 CFR 73.53, that the licensee must address through their cyber security program: latent – design basis threat (Category I FCF licensees only); latent – safeguards (Category II FCF licensees only); active – safety; and latent – safety and security.

- A latent – design basis threat consequence of concern can only occur at a licensee authorized to possess or use a formula quantity of strategic special nuclear material (i.e., Category I FCF licensee). Similar to the latent consequence of concern for safeguards, this concern involves the compromise of a security or safeguards function as a result of a cyber attack. The end result is that the function is compromised such that it cannot prevent radiological sabotage; theft or diversion of formula quantities of strategic special nuclear material; or the loss of nuclear material control and accounting for the aforementioned nuclear material. A latent consequence of concern for design basis threat potentially prevents a licensee from meeting the requirements of 10 CFR 73.1(a) or 74.51 during a secondary event.

- A latent – safeguards consequence of concern can only occur at a licensee authorized to possess or use special nuclear material of moderate strategic significance (i.e., Category II FCF licensee). This consequence of concern involves the compromise of a digital asset performing a security or safeguards function as a result of a cyber attack. This situation would in turn allow a malicious actor to exploit the degraded function to accomplish either the unauthorized removal of or the loss of nuclear material control and accounting for special nuclear material of moderate strategic significance.

- An active – safety consequence of concern has the potential to occur at any FCF licensee. This consequence of concern is directly caused by a cyber attack. In this situation, the cyber attack compromises a given digital asset. The function of that digital asset is manipulated, leading to the occurrence of one or more of the specified safety related results in Table C-1, Section 3. This manipulation can be intentional on the part of the attacker or unintentional.

- A latent – safety or security consequence of concern has the potential to occur at any FCF licensee. This consequence of concern is the compromise of a safety or security function by a cyber attack. The attack renders one or more digital assets incapable of performing its intended safety or security function. When called upon to respond due to a secondary event, separate from the cyber attack, the safety or security function does not operate as expected and in turn one or more of the consequence of concern in Table C-1, Section 4 occurs.

There are distinct differences between active and latent consequences of concern. For the active case, the compromise of the digital asset directly results in a radiological or chemical exposure exceeding the values in Table C-1, Section 3. In the latent case, a function is compromised, but there is no impact on safety, security, or safeguards until a secondary event occurs (i.e., an initiating event separate from the cyber attack). For the latent case, the compromised digital asset is no longer able to provide the function needed to prevent, mitigate, or respond to an initiating event. The combination of the compromise from the cyber attack, the resulting latent consequence of concern, and the secondary (i.e., initiating) event, must each occur for there to be a significant impact on public health and safety or the common defense and security.

Another difference between an active and latent consequence of concern is the time that typically elapses between the compromise of the digital asset and the event. An active consequence of concern leads directly to an event (e.g., radiological or chemical exposure). However, a latent consequence of concern requires a secondary event, separate from the effects of the cyber attack, before there is a consequence of concern. Therefore, the licensee may have the opportunity to identify the compromise caused by a latent consequence of concern and implement measures to prevent a consequence of concern before there is an impact on safety, security, or safeguards. For this reason, robust detection and response capabilities are important aspects of an adequate cyber security program. Conversely, for digital assets related to active consequences of concern, the cyber security controls and response efforts should account

for the direct relationship between a compromise and a consequence of concern, and the short time needed for a consequence of concern to result following the compromise.

Licensees should use the types of consequences of concern listed in Table C-1, Sections 1 through 4 as the starting point to determine what digital assets could be affected by a cyber attack and lead to a consequence of concern. The applicable types of consequence of concern depend on the facility classification as follows:

- Conversion and deconversion FCF licensees would consider:
  - Active – safety; and
  - Latent – safety and security.

- Category III FCF licensees would consider:
  - Active – safety; and
  - Latent – safety and security.

- Category II FCF licensees would consider:
  - Active – safety;
  - Latent – safety and security; and
  - Latent – safeguards.

- Category I FCF licensees would consider:
  - Active – safety;
  - Latent – safety and security; and
  - Latent – design basis threat.

In the case where a digital asset is associated with more than one consequence of concern, the licensee is expected to analyze the asset to determine if it is considered a VDA in regard to any of the associated types of consequence of concern. Additional guidance on the identification of digital assets and VDAs is provided in Chapter C, Section 6 of this document. Also, additional guidance on addressing the performance specifications of cyber security controls is provided in Chapter C, Section 7 of this document.

6 Identification of Digital Assets

The provision of 10 CFR 73.53 require licensees to identify and protect digital assets that, if compromised by a cyber attack, would cause a consequence of concern. Not all digital assets at a facility require protection. Therefore this RG provides one acceptable approach licensees may use to determine which digital assets: do not require any additional protection; can be protected by alternate means; or require cyber security controls. To accomplish this, the following three steps outline how to identify digital assets and VDAs at FCF licensees:

Step 1 – Identify digital assets associated with consequences of concern;

Step 2 – Identify VDAs by considering alternate means; and

Step 3 – Determine boundary and support systems for each VDA.

6.1 Identifying digital assets associated with a consequence of concern

Consistent with 10 CFR 73.53(d)(3), FCF licensees are required to identify digital assets that, if compromised by a cyber attack, would result in a consequence of concern. As defined in footnote 1 to this document, digital assets are electronic devices or organized collections of devices that either process information, communicate data, or are programmed to manipulate licensee site machinery. Examples of digital assets include, but are not limited to: computers and databases; switches and networks; programmable logic controllers; and industrial control systems. Additionally, as stated in 10 CFR 73.53(d)(3), licensees do not have to identify digital assets that are a part of a classified system accredited or authorized by another Federal agency under a formal security agreement with the NRC.

In order to develop an effective protection strategy, licensees must have in-depth knowledge of how digital assets affect their site operations that are associated with a consequence of concern. To gain this knowledge, licensees should:

- Identify site areas and processes associated with a consequence of concern.
- Examine those site areas and processes for 1) functions that could be compromised to directly cause a safety consequence of concern (i.e., active) or 2) functions needed to prevent a consequence of concern (i.e., latent).
- Examine those functions and identify the role of digital assets.
- Determine if the compromise of the digital asset would directly lead to a consequence of concern (i.e., active – safety). Additionally, determine if the compromise of the digital asset would lead to a consequence of concern if a secondary event occurred (i.e., latent – DBT, latent – safeguards, or latent – safety and security). To make these determinations, licensees should:
    - Review software platforms and applications related to those functions or processes.
    - Map organizational communication and data flows involving the digital assets.

If the compromise of the digital asset would lead to one or more of the aforementioned consequences of concern, then the digital asset is within the scope of 10 CFR 73.53 and must be further analyzed to determine if it is vital.

Licensees should, at a minimum, use the following resources to support the identification process:

- Integrated safety analyses (ISAs) and/or process hazards analyses;
- Physical security plan;
- Fundamental nuclear material control plan;
- Security orders;
- Previously considered impacts from a cyber attack;
- Site or system vulnerability analyses; or
- Other safety or security information.

Potential digital assets associated with a consequence of concern are likely to exist as part of a number of safety and security programs through the facility. Examples of systems that may contain digital assets related to a consequence of concern include:

- Items relied on for safety – potential active or latent safety consequences of concern;
- Plant features and procedures – potential active or latent safety consequences of concern;
- Intrusion detection systems (physical security) – potential latent security (for protection of classified information or matter), safeguards, or DBT consequences of concern;
- Material control and accounting database – potential latent safety, safeguards, or DBT consequences of concern.

In accordance with 10 CFR 73.53(i), a licensee must retain supporting documentation demonstrating compliance with the requirements of 10 CFR 73.53 as a record. Identification of digital assets that, if compromised by a cyber attack, would result in a consequence of concern is required by 10 CFR 73.53(d)(2). Licensees should document the following information (e.g., in a table or list), to identify all digital assets associated with a consequence of concern:

- The name and physical location of the application, device, system, or network identified as a digital asset; and
- Which of the four types of consequences of concern are potentially applicable if a compromise of the digital asset were to occur.

In accordance with 10 CFR 73.53(e)(3), site-specific analysis and other supporting technical information used by the licensee to support the development and implementation of the cyber security plan need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by the NRC staff.

6.2 Alternate means analysis

Once the licensee has identified those digital assets associated with a consequence of concern, the licensee is required by 10 CFR 73.53(d)(4) to determine which of those digital assets are vital. This analysis will determine if cyber security controls are required for the digital asset. In accordance with 10 CFR 73.53(d)(4), a digital asset is vital if no alternate means that is protected from a cyber attack can be credited to prevent the active consequence of concern or maintain the function needed to prevent the latent consequence of concern.

For this rule, the availability and usage of an alternate means is an equivalent substitute for implementing the measures taken to address the cyber security controls for digital assets associated with a consequence of concern. Licensees should look at the function of the digital asset to determine if an alternate means exists that could be credited or implemented to protect against a cyber attack capable of causing a consequence of concern.

When considering options during this detailed analysis, licensees should remember that an acceptable alternate means:

- Is protected from a cyber attack;

- Is sufficiently reliable and adequately implemented consistent with other safety features;
- Is properly maintained;
- Prevents the identified consequence of concern;
- Can be activated in a timely manner to prevent the identified consequence of concern;
- Would be implemented with available resources;
- Would not be adversely impacted by the potential multi-node cyber attack;
- Considers the cumulative effects from a cyber attack; and
- Does not contribute to other vulnerabilities or lead to a consequence of concern.

Examples of alternate means can include, but are not limited to:

- Physical barriers;
- Material holding tanks;
- Temperature, pressure and volume regulators or sensors;
- Flow control of material through the production process;
- Items relied on for safety [similar to plant features and procedures at some FCF licensees];
- Process monitoring equipment and procedures;
- Manual or automatic failsafe features or processes;
- Process stoppage in a timely manner before the consequence of concern can occur; or
- Other VDAs.

Licensees are allowed to credit a single alternate means for multiple digital assets to prevent a consequence of concern. An alternate means may be shared by multiple digital assets if it:

- Is adequate to perform the credited function(s);
- Is protected from a cyber attack; and
- Considers the potential cumulative effects from simultaneous compromise of the associated digital assets.

The licensee should consider factors which include availability, reliability, and capacity of the alternate means to perform the credited function(s). For example, a single security guard may not be able

to protect several different digital assets and their associated functions simultaneously. Conversely, the licensee could demonstrate that multiple attack vectors are not feasible.

Licensees should develop a detailed analysis that a resource can be credited as an alternate means. The licensee should assure that the alternate means prevents the consequence of concern. The documentation associated with alternate means accreditation is subject to inspection by the NRC.

Although the design or configuration of a digital asset may have some inherent protection (e.g., air-gapped, non-internet facing, stand alone, and protected by a firewall, data diode, virtual local area network, tunneling, or cross-domain solution), this is not an acceptable alternate means. An acceptable alternate means needs to address all cyber attack vectors for a given digital asset. The same concept applies to existing security features (e.g., access management, authentication, encryption, insider threat mitigation, media protection, monitoring, etc.), plant procedures, and other physical security activities that do not address all cyber attack vectors.

These configurations and security features may, however, provide measures that would address certain performance specifications of the cyber security controls required if the digital asset was determined to be a VDA. VDAs can be considered for use as an alternate means if they are protected from a cyber attack in accordance with 10 CFR 73.53(d)(5). Additional information on addressing the performance specifications of cyber security controls can be found in Chapter C, Section 7.2 of this document.

6.3 Vital digital assets

In accordance with 10 CFR 73.53(d)(4), any digital asset identified through 10 CFR 73.53(d)(3) that does not have an alternate means to prevent the consequence of concern is considered vital. As stated in 10 CFR 73.53(d)(5), VDAs are those devices or collections of devices that must be protected from cyber attack by addressing the performance specifications of the appropriate cyber security controls and establishing and maintaining written implementing procedures documenting the measures taken to address the cyber security controls.

The term VDA is inclusive of all components necessary to perform the function needed to prevent the consequence of concern. Multiple components may be considered a single VDA when a logical connection exists between their related equipment, technology, function, general operating environment, process, and direct operational and management control. Additionally, support systems (i.e., devices, utilities, or services) may contribute to the functionality of the VDA. Examples of support systems include, but are not limited to, electrical power; heating, ventilation, and air conditioning; communications; and fire suppression. Additional guidance on VDA boundaries and support systems is provided in Chapter C, Sections 6.3.1 and 6.3.2 of this document.

In the case where a VDA is associated with more than one consequence of concern, it is expected that the licensee would address the performance specifications of the more comprehensive cyber security controls specific to the applicable consequences of concern. Additional guidance on addressing the performance specifications of cyber security controls is provided in Chapter C, Section 7 of this document.

In accordance with 10 CFR 73.53(i), a licensee must retain supporting documentation demonstrating compliance with 10 CFR 73.53 as a record. Licensees should document the following information for all VDAs in written implementing procedures:

- A general description, including the physical and logical location, of each application, device, system, or network identified as a VDA;

- A brief description of the function(s) provided by the VDA, including which of the four types of consequences of concern are applicable if a compromise of the digital asset were to occur; and

- Identification of support systems for the VDA that, if compromised by a cyber attack, would cause the consequence(s) of concern.

Additional guidance on VDA documentation and the associated cyber security control implementing procedures is provided in Chapter C, Section 8 of this document.

6.3.1 Boundaries for vital digital assets

The term VDA is inclusive of all components necessary to perform the functions needed to prevent the consequence of concern. Multiple components (e.g., network) may be considered a single VDA when a logical connection exists between their related equipment, technology, function, general operating environment, process, and direct operational and management control. Conversely, a single component or network segment may be identified as a VDA.

The determination of the boundary is key to defining a VDA. The boundary is established by identifying the components that, together, provide the function(s) needed to prevent the consequence of concern. The boundary should be clearly defined to allow the licensee to protect the entire VDA by taking measures to address the performance specifications of the appropriate cyber security controls.

By defining the VDA's boundary, the licensee establishes the confines to take the measures to address the performance specifications of the appropriate cyber security controls. The VDA's boundary definition should be documented and, in accordance with 10 CFR 73.53(e)(3), this documentation is subject to inspection by the NRC.

6.3.2 Support systems for vital digital assets

Support systems are defined as resources (e.g., power, heating ventilation, air conditioning, communications, and data) necessary for the VDA to function properly. These systems can also include devices used for calibration and testing of VDAs (e.g., meters, laptops, smart phones). Licensees should consider the level of dependence between the VDA and its support systems to determine the impact a compromise of the support system could:

- Provide an input to a VDA that causes a consequence of concern;

- Directly cause a consequence of concern; or

- Preclude the VDA from performing the function needed to prevent a consequence of concern.

If any of the three conditions above are applicable, the provisions of 10 CFR 73.53(d)(5) require the identified support system to be protection from a cyber attack capable of resulting in a consequence of concern. This support system could be included within the boundary of the VDA or considered as a separate VDA. If a support system is used by more than one VDA, it is expected that the licensee would address the more comprehensive cyber security controls specific to the applicable consequences of

concern. Additional guidance on addressing the performance specifications of cyber security controls is provided in Chapter C, Section 7 of this document.

6.3.3 Grouping of vital digital assets

VDAs may be grouped to more efficiently address cyber security controls. They may be defined individually; alternatively, similar VDAs throughout the facility may be addressed as a group, so long as controls can be applied equally to address the associated consequences of concern.

Grouping is different from defining a boundary. This does not mean that a common boundary is defined. Under these conditions, one implementing procedure may be applied to the entire group to facilitate documenting the measures taken to address the performance specifications of the appropriate cyber security controls. Grouping of VDAs should be noted in the documentation associated with the digital asset identification process. In accordance with 10 CFR 73.53(e)(3), this documentation is subject to inspection by the NRC.

7 Cyber Security Controls

A cyber security control is a performance specification established to provide an element of protection from specific cyber attack vectors. The performance specification of a cyber security control is satisfied by taking measures to address the cyber attack vector(s). In order to effectively protect VDAs against cyber attacks associated with a consequence of concern, FCF licensees are required to establish and maintain cyber security controls in accordance with 10 CFR 73.53(d)(2). The provisions of 10 CFR 73.53(d)(5) require measures be taken and documented to address the performance specifications of the appropriate cyber security controls. Cyber security controls for the specific types of consequences of concern are required by 10 CFR 73.53(e)(1) to be documented in the licensee's cyber security plan.

7.1 Standards and applicable cyber security controls

The NRC has developed the technical cyber security controls in Appendices B through F of this RG, which may be used by licensees to meet the requirements of 10 CFR 73.53(d)(2). These cyber security controls are informed by the NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision (Rev.) 4 (Ref. 10) and NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," Rev. 2 (Ref. 11). In addition, the NRC used its own cyber security guidance for nuclear power reactors (RG 5.71) as a source of reference for developing controls for FCF licensees. Further, the NRC has modeled its expectations for FCF licensees after NIST's "Framework for Improving Critical Infrastructure Cyber Security," Version 1 (Ref. 12), and its "Manufacturing Profile," draft, April 2016 (Ref. 13).

The licensee's cyber security plan should identify the guidance or standard(s) (e.g., this RG, NIST, ISO/IEC) that the licensee will use to establish and maintain cyber security controls, in accordance with 10 CFR 73.53(d)(2). The cyber security controls should be documented in the cyber security plan, similar to the template in Appendix A, "Cyber Security Template."

7.2 Establishing cyber security controls and addressing performance specifications

In accordance with 10 CFR 73.53(d)(3) and (4), the licensee must determine the type of consequence of concern that could result if each VDA is compromised. Taking measures for VDAs to address the performance specification of the appropriate cyber security controls and documenting the associated implementing procedures is required by 73.53(d)(5). To satisfy this requirement, the licensee can utilize the controls listed in the appendices provided as part of this RG for each applicable

consequence of concern (i.e., address the performance specifications of: 1) the controls that are associated with all VDAs; and 2) the controls associated with the specific type of consequence of concern). A licensee may also utilize equivalent controls. The licensee should document in the VDA's implementing procedure for how these controls are addressed. The documentation should demonstrate that the controls are adequate to prevent the consequence of concern. Additional guidance on implementing procedures is provided in Chapter C, Section 8 of this document.

A cyber security control is a performance specification established to provide an element of protection from specific cyber attack vectors. The NRC has developed cyber security controls for use by FCF licensees as listed below:

- Appendix B, "Cyber Security Controls for Vital Digital Assets Associated with any Consequence of Concern," which is applicable for all types of FCF licensees;

- Appendix C, "Additional Cyber Security Controls for Vital Digital Assets Associated with Latent Consequences of Concern – Design Basis Threat (Category I Facilities Only);"

- Appendix D, "Additional Cyber Security Controls for Vital Digital Assets Associated with Latent Consequences of Concern – Safeguards (Category II Facilities Only);"

- Appendix E, "Additional Cyber Security Controls for Vital Digital Assets Associated with Active Consequences of Concern – Safety," which is applicable for all types of FCF licensees; and

- Appendix F, "Additional Cyber Security Controls for Vital Digital Assets Associated with Latent Consequences of Concern – Safety and Security," which is applicable for all types of FCF licensees.

If a licensee adopts the cyber security controls from the referenced Appendices, the licensee should address each cyber security control applicable to the type of consequence of concern associated with each VDA.

If the licensee elects to use a different set of controls in accordance with 10 CFR 73.53(d)(2) and (e)(1), the licensee will be responsible for:

- Developing cyber security controls specific to the applicable types of consequence of concern;

- Establishing their performance specifications to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern; and

- Documenting the controls in the cyber security plan.

While Appendix B contains cyber security controls that are applicable to all VDAs, Appendices C-F are graded based on the consequence of concern in order of most to least comprehensive cyber security controls: 1) Appendix C; 2) Appendix D; 3) Appendix E; and 4) Appendix F). Therefore, by addressing the cyber security controls from Appendix C, a licensee would also satisfy the controls in Appendices D, E, and F. If a licensee adopts the cyber security controls from the referenced Appendices, the licensee is expected to use the more comprehensive cyber security controls when more than one consequence of concern is possible for a VDA.

This graded comprehensiveness may not be present if a licensee elects to use a different set of controls. In this case, when more than one consequence of concern is possible, the licensee could either address the controls for all applicable consequences of concern or demonstrate that the more comprehensive controls are sufficient.

The performance specification of a cyber security control is addressed by taking measures to protect against specific cyber attack vector(s). A measure is an item or action (e.g., computer hardware, software, plant procedures) that provides protection from a cyber attack vector and addresses the performance specifications of a cyber security control. A single measure may not be sufficiently robust to adequately provide protection from the specific cyber attack vector in its entirety. Therefore, addressing the performance specifications of a cyber security control may involve various measures that are needed in combination.

Licensees should recognize that each control must be addressed individually. Furthermore, a cyber security control should not be considered satisfied by a measure taken to address another cyber security control for the same VDA, unless both controls are specifying protection from identical cyber attack vectors (e.g., the protection provided by a firewall does not address a cyber security control with a performance specification for encryption).

The specific cyber security controls applicable to a VDA are derived from the controls established through 10 CFR 73.54(d)(2) and documented in the cyber security plan. The cyber security controls that must be addressed are determined by the type(s) of consequence of concern(s) associated with the VDA under consideration. In accordance with 10 CFR 73.53(d)(5) and (e)(2), the licensee must document how each cyber security control was addressed in the implementing procedure associated with the VDA and maintain those records available for inspection by the NRC.

A licensee may determine that one or more of the cyber security controls documented in the cyber security plan for a given type of consequence of concern should not be applied to a VDA, or to the cyber security program as a whole. To address the control, in this case, the licensee should document the justification for not taking measures. Justifications can include site-specific issues (e.g., the technical control cannot be adopted by a particular VDA because the asset cannot support it physically) as well as operational choices by the licensee (e.g., media protection is not required as all media access points for VDAs have been removed). The justification should demonstrate how the equivalent protection of a VDA, or effective operation of the cyber security program, is achieved without the application of additional measures to address a particular performance specification of the cyber security control.

7.2.1 Cyber security control parameters

The cyber security controls provided in the Appendices to this RG were developed by specifying parameters (i.e., assignment and selection statements) to clarify the performance specifications of the controls and enhancements to support application to VDAs. Licensees developing their own cyber security controls should clearly define and record similar parameters and maintain this documentation for inspection by the NRC.

7.2.2 Tailoring of cyber security controls for specific vital digital assets

Tailoring is defined as the modification of a cyber security control's performance specifications or parameters to fit a given condition for a specific VDA. Controls should not be tailored solely for operational convenience. Tailoring decisions regarding controls should be defensible based on attributes of the VDA under consideration. Decisions can also be based on timing and applicability of selected controls under certain defined conditions. That is, the performance specifications of a control may not

apply in every situation or the control's parameter values may need to be changed based on VDA specific conditions. Tailoring decisions, including the specific rationale for those decisions, should be documented in the implementing procedures. Every control established for the applicable consequence of concern should be accounted for and addressed. If certain cyber security controls are tailored, then the associated rationale should be recorded in the implementing procedures (or references/pointers to other relevant documentation are provided) for the VDA under consideration and is subject to inspection by the NRC staff.

7.2.3 Common cyber security controls

When addressing controls for a VDA, it is possible for licensees to take credit for controls already in place for related assets or to group assets under the protection of a given established control. This is defined as a common control. The use of common controls may reduce the number of controls specifically implemented for that VDA. This in turn reduces the administrative effort in satisfying controls as well as developing implementing procedures. Common controls can be used for all VDAs or certain groups of VDAs. It is up to the licensee to determine, based on site characteristics, where common controls and their associated measures can be utilized. It is expected that the use of common controls would be documented in the appropriate implementing procedures, which should provide traceability to the source document in which the controls are originally referenced.

7.2.4 Inherited cyber security controls

A cyber security control can be inherited for a subordinate VDA by crediting specific cyber security measures taken for a parent VDA. The inherited control would not need to be explicitly implemented on the subordinate VDA, the implementing procedure would simply reference the parent VDA's control. Unlike common controls, this refers to a specific one-to-one relationship between two VDAs. Again, it is expected that inherited controls would be documented in the appropriate implementing procedures. This will provide traceability to the VDA where the control is originally applied.

7.3 Verifying cyber security controls

After the measures have been taken to address the performance specifications associated with the cyber security controls for a VDA, the licensee should perform a controls assessment. This assessment should consider the cyber security controls for the VDA and its environment of operation, to determine the extent to which the associated measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established performance specifications. The individuals assessing the controls should be different than those who applied the measures. The implementing procedure documenting the measures taken to address the performance specifications for the controls applicable to each VDA should describe the conditions under which this assessment will be conducted, the frequency, and roles and responsibilities for the team conducting the assessment. Licensees should document the results and keep them available for inspection by the NRC.

In conjunction with the controls assessment, the licensee should review the interconnections between a VDA and other systems, devices or networks. At a minimum it is expected that the licensee through its cyber security program would analyze and document for each interconnection the interface characteristics, security requirements, and the nature of the information communicated. These considerations would prohibit unauthorized interconnections to VDAs and assist in confirming that support systems have been properly identified.

The results of the controls and VDA assessments should be reviewed by the CST. Should the assessments show that all controls have been effectively implemented, then the CST Program Manager or Program Sponsor should document that the controls applied to the VDA are acceptable to protect against a consequence of concern. However, for those solutions or features that do not effectively address one or more controls, the licensee should remediate the weaknesses of the controls or deficiencies noted during the assessment. At this point, the licensee can choose to not operate the VDA and rework its solution for protecting against a consequence of concern until it can be successfully confirmed though assessment. Otherwise the licensee can also choose to utilize an interim compensatory measure to operate the VDA until the required solution can be reworked and assessed.

7.4 Cyber security control maintenance

Licensees should maintain their cyber security controls up to date, as a part of their overall cyber security program, so they remain applicable to existing conditions at the facility. New cyber security controls, control enhancements, or modifications to existing controls should be developed as needed based on latest state-of-the-practice information from national-level threat and vulnerability databases as well as information on the tactics, techniques, and procedures employed by adversaries in launching cyber attacks. Cyber security controls are part of the cyber security plan, therefore additions, modifications, or changes that would result in a decrease in the effectiveness of a cyber security control must be submitted to the NRC in accordance with 10 CFR 40.32(h) or 10 CFR 70.32(f), whichever is applicable to the specific FCF licensee, for review and approval prior to implementation.

8 Implementing Procedures and Interim Compensatory Measures

Consistent with requirements in 10 CFR 73.53(d)(5)(ii), the licensee must establish and maintain written implementing procedures for VDAs. These implementing procedures document the measures taken to address the performance specifications associated with the identified cyber security controls. The licensee should analyze each VDA to determine and document the applicable cyber security controls. The implementing procedures should also describe the testing required to confirm that the measures address the performance specifications of the associated controls.

In accordance with 10 CFR 73.53(d)(6), licensees must implement interim compensatory measures when the measures taken to address the performance specifications of the controls fail to provide meet the cyber security program performance objectives. Licensees should ensure they document and track to completion the interim compensatory measures when they are used to protect a VDA.

An example of an implementing procedure is available in Appendix G of this guidance document.

8.1 Implementing procedures

Implementing procedures should identify and document the cyber security controls applicable to the VDA(s). Licensees may reference existing procedures to avoid redundancy. At a minimum the implementing procedures should document the following information:

8.1.1 Identification of the vital digital asset and boundary

The procedure should identify the VDA by describing its major components (e.g., computers, logic controllers, network communication devices, storage devices) within the defined boundary.

8.1.2 Consequence of concern type

The procedure should identify the type(s) of consequence of concern associated with the VDA based on the analysis performed by the licensee.

8.1.3 Function, general description, and purpose of the vital digital asset

The procedure should identify if the VDA is performing a safety, security, or safeguards function. It should also include a general description and the VDA's purpose.

8.1.4 Individual(s) or organization responsible for the VDA

The procedure should identify the individual(s) by job title or role (e.g., Security Manager) or organization (e.g., Security Department) responsible for the VDA. If several VDAs are combined into a group and the responsibilities are spread among several individuals or organizations, the procedure should list the individual(s) or organization(s) responsible for each VDA.

8.1.5 Location, interconnections, and environment

The procedure should identify the physical or network location of the VDA and relevant information concerning the operating environment (e.g., network and client operating system, communications protocol). The procedure should include a network diagram showing the VDA's interconnections and defined boundaries. Licensees may reference network diagrams in existing procedures to avoid redundancy.

8.1.6 Support systems

If applicable, the procedure should identify support systems associated with the VDA based on the analysis performed by the licensee, see Chapter C, Section 6.3.2 of this guidance document for additional information. The procedure should describe the VDA's reliance on the support system. If the support system is identified as a separate VDA, then its implementing procedure should be referenced.

8.1.7 Tools

When appropriate, the procedure should identify tools used in the operation, calibration, or maintenance of the VDA.

8.1.8 Inventory

The procedure should list an inventory of the VDA components (e.g., hardware, peripherals, firmware, and software) necessary to support configuration management.

8.1.9 Addressing and validating cyber security controls.

The controls associated with a VDA are addressed and validated through the implementing procedure. The procedure documents the measures taken to meet the performance specifications associated with the identified cyber security controls. For each control, the licensee:

- Takes new measures to meet the performance specifications outlined in the control;
- Uses existing measures to meet the performance specifications outlined in the control; or

- Provides a justification that the control is not applicable to the VDA.

If the licensee determines that a new measure is required, the licensee evaluates the control to identify the performance specification. Then the CST will identify the measure(s) needed to protect the VDA. Once the licensee has selected the measure(s), they develop and document the measure's expected performance in the implementing procedure. Licensees should ensure that proper configuration management is performed. When taking new measures, cyber security controls are validated through testing (e.g., vulnerability scanning, table top exercises).

If the licensee determines an existing measure will be used, the licensee evaluates the control to identify the performance specification. Then the CST will identify the measure(s) needed to protect the VDA. Once the licensee has selected the measure(s), they develop and document through reference the measure's expected performance in the implementing procedure. When using existing measures, cyber security controls are validated through confirmation of applicability to the VDA.

If the licensee determines a control is not applicable, they document a justification demonstrating protection from the cyber attack vector(s) associated with the control's performance specifications. This justification may range from the simple recognition that the cyber attack vector does not exist, to a detailed analysis. When providing a justification that the control is not applicable, validation is not required.

8.1.10 Grouping VDAs and common or inherited controls.

If the VDAs are grouped, one implementing procedure may be applied to the entire group to address the cyber security controls. This has the advantage of reducing paperwork by documenting identical measures taken to address controls. Grouping of VDAs, as noted in the documentation associated with the digital asset identification process, should be referenced or described in the implementing procedure.

If the VDA uses a common or inherited control, the implementing procedure should reference the source document in which the controls are originally described. This has the advantage of reducing the burden of taking multiple measures to VDAs that are already protected by the common or inherited control. To maintain traceability, the use of common or inherited controls should be referenced in the appropriate implementing procedures.

8.2 Interim compensatory measures

If after an implementing procedure has been completed and the intended measure does not meet the performance specifications of the control, licensees are required by 10 CFR 73.53(d)(6) to implement interim compensatory measure(s). An interim compensatory measure (ICM) is a temporary solution to replace a measure(s) used to address one or more cyber security controls and the associated performance specifications. These are time limited solutions that allow the VDA to be operated while the long term method to address the control is properly implemented and verified. The ICM must be documented and tracked to completion.

The licensee should document the function of the ICM, how it will address the control effectively, and the timetable for the modification of the intended measure. The licensee should document, at regular intervals, progress on implementing a long term solution and ensure the issue is tracked to completion. Licensees should document justification and appropriate management approval for an ICM that would be kept in use for more than one calendar year from the date of adoption.

ICMs should be employed as necessary for VDAs if measures fail to provide protection from the cyber attack vectors(s) associated with the performance specifications of the corresponding cyber security control. The configuration management system required under 10 CFR 73.53(f) may identify new or modified measures implemented through procedures, which may require ICMs. Furthermore, the periodic review process required under 10 CFR 73.53(g) may identify findings, deficiencies, and recommendations, which may require ICMs.

9 Configuration Management

After the licensee has fully implemented the cyber security program by identifying and protecting its VDAs, 10 CFR 73.53(f) requires that a configuration management system be utilized to ensure that changes to the facility are properly evaluated. This system ensures that changes (e.g., addition, modification, or removal of devices and equipment) are evaluated prior to implementation and do not adversely impact the licensee's ability to meet the cyber security program objectives. This system must be documented in written procedures and can be added to an existing site design, configuration management, or improvement program.

The system should establish the appropriate procedures for documenting the evaluation and approval of additions or changes associated with digital assets and VDAs. Evaluating additions or changes may take the form of a cyber security impact analysis (impact analysis). When properly implemented, the configuration management system should protect against improper or unintended changes to the cyber security program. Furthermore, the licensee should consider a site-wide approach by incorporating cyber security configuration management into the planning process for the facility.

9.1 Cyber security impact analysis

An acceptable way for licensees to address configuration management for cyber security is to conduct a cyber security impact analysis as a part of a proposed change. A cyber security impact analysis examines the proposed change to determine if it could introduce vulnerabilities allowing a cyber attack to result in a consequence of concern. This impact analysis assists in managing potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats.

The cyber security impact analysis should identify adjustments or actions affecting the cyber security program as a result of the proposed change. The effort would also determine if existing alternate means and measures taken to address cyber security controls would be affected or degraded by the proposed change. Additionally, this impact analysis would determine if adjustments would be required to maintain the effectiveness of the existing detection process or implementing procedures. Furthermore, this impact analysis would consider the potential effects that the proposed change would have on the cyber security plan, cyber security incident response (CSIR) procedures, other documentation, or processes.

Before making a design or configuration change to a VDA or when changes to the environment occur, at a minimum, a licensee should demonstrate that the proposed change: 1) does not introduce unaddressed cyber security vulnerabilities that would allow a cyber attack to result in a consequence of concern; and 2) maintains the protection established by the measures taken to address controls, detection schemes, and the availability of alternate means. At the completion of the analysis, a licensee may need to address cyber security vulnerabilities identified in the analysis, as required by 10 CFR 73.53(d).

9.2 Site-wide considerations

The results of a cyber security impact analysis, revisions to implementing procedures, and other applicable considerations developed by the CST should be shared with the appropriate facility design and operations functions. The CST should work with their counterparts throughout facility operations to ensure that the implementing procedures are properly executed. Changes as a result of the procedure should be tested and verified before use in the licensee's production environment. The overall process, digital asset, or VDA should not be considered sufficiently protected until: the implementing procedure has been completed and validated; and the corresponding measures have been taken to address the performance specifications of the cyber security controls. Interim compensatory measures can be employed as needed should the new implementing procedure proves inadequate.

The CST should also consider how VDAs are authorized to operate after controls are addressed and verified due to changes to the licensee's environment or digital assets. This would include incorporating and validating changes to documentation or other implementing procedures to reflect adjustments to cyber security controls or their associated measures. Consistent with 10 CFR 40.32(h) or 10 CFR 70.32(f), amendments to the cyber security plan that would result in a decrease in the effectiveness of the cyber security program must be submitted to the NRC for review and approval prior to implementation of the change. In addition, the VDA authorization process itself should be incorporated in the procedures for the configuration management system.

Through the configuration management system, the licensee should implement a process for ensuring that cyber security testing, training, and monitoring activities associated with VDAs are properly maintained. The CST should confirm that these actions continue to be executed in a timely manner are consistent with the cyber security plan as changes occur to the facility, digital assets, and VDAs.

10 Review of the Cyber Security Program

In accordance with 10 CFR 73.53(g), the licensee should perform a review of the cyber security program. The periodic review serves to evaluate the overall effectiveness of the cyber security program. Licensees authorized to possess or use a formula quantity of strategic special nuclear material must perform a review of the cyber security program as a component of the security program in accordance with the requirements of §73.46(g)(6), including the periodicity requirements. All other licensees must perform a review of the cyber security program at least every 36 months.

An acceptable approach includes an audit of the effectiveness and adequacy of the cyber security program including, but not limited to review of:

- The purpose, scope, roles, responsibilities, requirements, and management commitments of the cyber security program;
- The measures of performance established through cyber security controls and develop, monitor, and report on the results these measures of performance;
- The cyber security control strategy;
- The use of alternate means and defensive architecture for digital assets;
- The facility's CSIR capability;

- The configuration management system; and

- The changes made to the operating environment.

The licensee should develop and implement procedures to facilitate and maintain the periodic review. These reviews should be completed by individuals independent of those personnel responsible for cyber security program management or implementation.

When the review is completed, the licensee must track, address in a timely manner, and document the findings, deficiencies and recommendations resulting from the review in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operations. This report should also include management's findings regarding cyber security program effectiveness and actions taken as a result of recommendations from prior cyber security program reviews. The licensee should maintain reports in an auditable format and make them available, upon request, for inspection by the NRC. The results of the periodic review may trigger the following changes to:

- The cyber security plan;

- The cyber security controls;

- The CSIR; and

- The implementing procedures for VDAs and associated controls.

Consistent with 10 CFR 40.32(h) or 10 CFR 70.32(f) a change to the cyber security plan, including the cyber security controls, that would result in a decrease in the effectiveness must be submitted to the NRC for review and approval prior to implementation of the change. The licensee may make changes to the cyber security plan without prior Commission approval if these changes do not decrease the effectiveness of the plan.

11 Event Reporting and Tracking

The reporting requirements located in 10 CFR 73.53(h) have two distinct concepts. First, licensees are required to inform the NRC Operations Center within 1 hour of discovery that an event requiring notification under existing regulations is the result of a cyber attack. This would not necessarily require licensees to initiate a separate report to the NRC; rather, licensees could add cyber security information to reports required for compliance with other regulations, if applicable. However, a second (or updated) report would be required if the licensee discovers later (i.e., after the initial reporting) that the reported event was the result of a cyber attack. Secondly, 10 CFR 73.53(h) requires that the following events need to be recorded within 24 hours of discovery and tracked to resolution:

- A failure, compromise, discovered vulnerability, or degradation that results in the decrease in effectiveness of a cyber security control identified through 10 CFR 73.53(d)(5); or

- A cyber attack that compromises a VDA associated with a consequence of concern identified in 10 CFR 73.53(c)(1)(iii) and (c)(2)(ii).

Although these events need to be recorded and tracked to resolution, the documentation is maintained by the licensee on site. No report need be submitted to the NRC, although the documentation

must be available for NRC inspection. The types of events that must be documented include: (1) a system, component, or cyber security control has been compromised to the degree that it is rendered ineffective for the intended purpose (e.g., cessation of proper functioning); (2) a defect in equipment, personnel, or procedure that degrades the function or performance of the cyber security program necessary to meet the requirements of 10 CFR 73.53; or (3) a feature or attribute in a system's design, implementation, operation, or management that could render a VDA open to exploitation.

Licensees are permitted and encouraged to voluntarily report cyber-related events or conditions that do not meet the criteria for required reporting, if the licensee believes that the event or condition might be of safety or security significance or of generic interest or concern. Assurance of safe operation depends on accurate and complete reporting by each licensee of events that have potential safety/security significance. For example, a cyber-related event or condition identified and mitigated outside the plant network with no impact on safety/security functions may be indicative of a recently identified or known cyber threat. Such activities should be voluntarily reported during NRC inspection to support Federal situational awareness activities.

12 Recordkeeping

In accordance with 10 CFR 73.53(i), the licensee must retain all records and supporting technical documentation required to satisfy the implementation of this regulation until the Commission terminates the license for which the records were developed. Furthermore, the licensee must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

An acceptable method for complying with this requirement is for the licensee to maintain records or supporting technical documentation so that inspectors, auditors, or assessors will have the ability to evaluate incidents, events, and other activities that are related to the cyber security elements described, referenced, and contained within the licensee's NRC approved cyber security plan. Cyber security program reviews and cyber security event reports should be maintained and available for inspection, for a period of three years.

D. IMPLEMENTATION

The purpose of this chapter is to provide information on how licensees[2] may use this guide and information regarding the NRC's plans for using this RG. In addition, it describes how the NRC staff complies with 10 CFR 70.76, "Backfitting."

Use by Licensees

Licensees may voluntarily[3] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this RG may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged**.**

Licensees may use the information in this RG for actions which do not require NRC review and approval such as changes to a facility design under 10 CFR 70.72, "Facility changes and change process." Licensees may use the information in this RG or applicable parts to resolve regulatory or inspection issues.

Use by the NRC Staff

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this RG. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this RG, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request licensees to voluntarily adopt this RG to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action which would require the use of this RG. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of this RG, requests for information under 10 CFR 70.22(d) as to whether a licensee intends to commit to use of this RG, generic communication, or promulgation of a rule requiring the use of this RG without further backfit consideration.

During regulatory discussions on plant specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this RG, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this RG are part of the licensing basis of the facility. However, unless this RG is part of the licensing basis for a facility, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this RG constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised RG and (2) the specific subject matter of this RG is an essential consideration in the staff's determination of the acceptability of the licensee's request, then the staff may request that the licensee either follow the guidance in this RG or provide an equivalent alternative process that demonstrates compliance with the

---

2 In this section, "licensees" refers to applicants for and holders of FCF licenses through 10 CFR Section 40.31 or 70.22.

3 In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 70.76(a)(1).

If a licensee believes that the NRC is either using this RG or requesting or requiring the licensee to implement the methods or processes in this RG in a manner inconsistent with the discussion in this Implementation chapter, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409, "Backfitting Guidelines," (Ref. 14) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 15).

GLOSSARY

alternate means	An available and reliable feature that is protected from a cyber attack and is credited, in lieu of cyber security controls, to prevent a specific consequence of concern associated with a digital asset.
common control	Cyber security controls in place for related vital digital assets. Note that similar vital digital assets with common controls may also have shared implementing procedures.
consequence of concern	Specific results of a cyber attack that a licensee must protect against.
cyber attack	The manifestation of physical, electronic, or digital threats against computers, communication systems, or networks that may: (1) originate from either inside or outside the licensee's facility, (2) utilize internal and/or external components, (3) involve physical, electronic, or digital threats, (4) be directed or non-directed in nature, (5) be conducted by threat agents having either malicious or non-malicious intent, and (6) have the potential to result in a consequence of concern.
cyber attack vector	The pathway or means of delivering (direction) a cyber attack's payload, exploit, or outcome (magnitude).
cyber security control	Performance specifications used to inform the measures taken to detect, protect against, or respond to a cyber attack capable of causing a consequence of concern.
cyber security incident response	The measures to respond to a cyber attack capable of causing a consequence of concern. Note that these measures would be taken prior to a consequence of concern occurring and would be documented in the licensee's cyber security incident response plan. Measures taken in response to a consequence of concern would be captured in the licensee's emergency plan.
cyber security plan	A document, referenced in the NRC license, that: (1) is established, implemented, and maintained by the licensee; (2) describes how the cyber security program performance objectives are met; and (3) accounts for site-specific conditions.
cyber security program performance objectives	Establish, implement, and maintain a cyber security program that will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern.
Cyber Security Team	A group of individuals that is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program.
digital asset	An electronic device or organized collection of devices that either process information, communicate data, or are programmed to manipulate licensee site machinery.
grouping of vital digital assets	Similar vital digital assets throughout the facility may be addressed as a group, so long as controls can be applied equally to address the associated consequences of concern. Note that one implementing procedure may be applied to a group of vital digital assets to facilitate the documentation of measures taken to address the performance specifications of the appropriate cyber security controls.
implementing procedure	Documentation of the measures taken for a vital digital asset to address the performance specifications of the applicable cyber security controls.

inherited control	A specific cyber security measure taken for parent vital digital asset that is credited by a subordinate vital digital asset to address the performance specification of a cyber security control. The inherited control would not need to be explicitly implemented on the subordinate vital digital asset, the implementing procedure would simply reference the parent vital digital asset's control. Unlike common controls, this refers to a specific one-to-one relationship between two vital digital assets.
measure	A capability, item, or action (e.g., computer hardware, software, plant procedures) that provides protection from a cyber attack vector and is taken to address the performance specifications of a cyber security control.
parameter	A specific value assigned to the performance specification of a cyber security control.
performance specification	A requirement established to provide a given level of protection against a specific cyber attack vector.
support system	Resources (e.g., power, heating, ventilation, air conditioning, communications, data) necessary for a vital digital asset to function properly. A support system may also be a device (e.g., meter, laptop, smart phone) used for calibration and testing a vital digital asset. A support system must be protected if its compromise could: (1) directly cause a consequence of concern; (2) provide an input to a vital digital asset that causes a consequence of concern; or (3) preclude the vital digital asset from performing the function needed to prevent a consequence of concern.
tailoring of a control	The modification of a cyber security control's performance specifications or parameters to fit a given condition for a specific vial digital asset.
vital digital asset	A digital asset for which no alternate means has been identified to prevent the associated consequence of concern.

REFERENCES[4]

1. U.S. Nuclear Regulatory Commission (NRC), "Design Basis Threat" *Federal Register*, Vol. 72, No. 52: pp. 12705, (72 FR 12705), Washington, DC, March 19, 2007. (74 FR 13926)

2. NRC, "Design Basis Threat" *Federal Register*, Vol. 74, No. 58: pp. 13926, (74 FR 13926), Washington, DC, March 27, 2009.

3. NRC, Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

4. NRC, SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," Washington, DC, June 25, 2012. (ADAMS No.: ML12135A050)

5. International Atomic Energy Agency (IAEA) Nuclear Security Series No.: 17, "Computer Security at Nuclear Facilities," Vienna, Austria, 2011.[5]

6. IAEA Nuclear Security Series No.: 23-G, "Implementing Guide for Security of Nuclear Information," Vienna, Austria, 2015.

7. IAEA Nuclear Security Series Technical Report No.: NP-T-1.13, "Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants," Vienna, Austria, 2015.

8. Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27000 Series, "Information Security Management System (ISMS), Family of Standards," Geneva, Switzerland, 2016.[6]

9. ISO/IEC 15408, "The Common Criteria for Information Technology Security Evaluation," Geneva, Switzerland, 2012.

   NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," Rev. 2, Gaithersburg, MD, May 2015.

---

4 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at: http://www.nrc.gov/reading-rm/adams.html The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at: 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov.

5 Copies of IAEA documents may be obtained through their Web site: www.IAEA.org/ or by writing the International Atomic Energy Agency, P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria.

6 Copies of ISO/IEC documents may be obtained through their Web site: http://standards.iso.org/ittf/PubliclyAvailableStandards/ or by writing the International Organization for Standardization, ISO Central Secretariat, BIBC II, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland.

10. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision (Rev.) 4, Gaithersburg, MD, April 2013.[7]

11. NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," Rev. 2, Gaithersburg, MD, May 2015.

12. NIST, "Framework for Improving Critical Infrastructure Cyber Security," Version 1, Gaithersburg, MD, February 2014.

13. NIST, "Manufacturing Profile," Draft, Gaithersburg, MD, April 2016.

14. NRC, "Backfitting Guidelines," NUREG–1409, Rev. 2, Washington, DC, July 1990. (ADAMS No.: ML032230247)

15. NRC, Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," Washington, DC, October 9, 2013. (ADAMS No.: ML12059A460)

7 Copies of NIST computer security documents may be obtained through their Web site: http://csrc.nist.gov/publications or by writing the National Institute of Standards and Technology, Attn: Computer Security Division, Information Technology Laboratory, 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930.

APPENDIX A

CYBER SECURITY PLAN TEMPLATE

CYBER SECURITY PLAN

FOR THE

[NAME] FACILITY

AT

[INSERT LOCATION]

TABLE OF CONTENTS

[PROVIDE A TABLE OF CONTENTS]

GLOSSARY AND ACRONYM LIST

[PROVIDE A LIST OF ACRONYMS USED WITHIN THE DOCUMENT]

APPENDIX A CYBER SECURITY PLAN TEMPLATE

CHAPTER 1 CONTENTS OF THE CYBER SECURITY PLAN

This Cyber Security Plan (CSP or Plan) is submitted by [FULL NAME], (hereafter called [NAME]) to the U.S. Nuclear Regulatory Commission (NRC) to satisfy the requirements of 10 CFR 73.53. The information in the Plan demonstrates that the cyber security program provides adequate compliance with the requirements for licensing to [STATEMENT OF LICENSED ACTIVITY]. This document is solely for the use of the NRC and [LICENSEE OR APPLICANT]. All information in this document and subsequent revisions is to be withheld from public disclosure in accordance with the provisions of 10 CFR 2.790(d) as this information identifies [LICENSEE OR APPLICANT] procedures for [LICENSED ACTIVITY].

The cyber security program satisfies the general performance objectives and recordkeeping requirements of 10 CFR 73.53. Details of this program are discussed in Plan Chapters 2 through 10. Additional description of the process and special authorizations are given in the [LICENSING DOCUMENTATION].

CHAPTER 2 DESCRIPTION OF THE CYBER SECURITY PROGRAM FOR THE [NAME]

2.1 INTRODUCTION

This cyber security plan contains commitments for [NAME] to establish, implement, and maintain a cyber security program adequate to meet the performance objectives in 10 CFR 73.53 to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The cyber security program is designed to detect cyber attacks directed towards vital digital assets. The detection process includes multiple data collection points, in-depth analysis mechanisms, and appropriate threat intelligence. Protection is accomplished by taking measures for vital digital assets to address the performance specifications of cyber security controls that have been established to protect against a specific consequence of concern. To remain effective, this protection must be monitored and maintained. In addition, [NAME] will implement compensatory measures to protect vital digital assets in the event cyber security controls fail, become degraded, or are not operating as intended. [NAME] will maintain the capability to respond to a cyber attack capable of causing a consequence of concern. A cyber security incident response (CSIR) plan [PROVIDE REFERENCE TO SEPARATE DOCUMENT OR APPLICABLE SECTION OF THIS DOCUMENT] will be maintained onsite to identify the specific steps and actions to respond to a cyber attack. The CSIR plan describes the structure and organization of the CSIR capability and defines the resources and management support committed to effectively maintain this capability.

2.2 PERFORMANCE OBJECTIVES

[PROVIDE AN OVERVIEW OF HOW THE PROGRAM WILL DETECT A CYBER ATTACK CAPABLE OF CAUSING A CONSEQUENCE OF CONCERN.]

[PROVIDE AN OVERVIEW OF HOW THE PROGRAM WILL PROTECT AGAINST A CYBER ATTACK CAPABLE OF CAUSING A CONSEQUENCE OF CONCERN.]

[PROVIDE AN OVERVIEW OF HOW THE PROGRAM WILL RESPOND TO A CYBER ATTACK CAPABLE OF CAUSING A CONSEQUENCE OF CONCERN.]

2.3 AFFIRMATIONS

[NAME] affirms the following with respect to the cyber security program:

- A cyber security program will be developed and maintained that will detect, protect against, and respond to a cyber attack capable of causing a consequence of concern as identified in 10 CFR 73.53(c).
- A cyber security team will be established and maintained that is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program consistent with 10 CFR 73.53(d)(1).
- Cyber security controls will be established and maintained that provide performance specifications to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern, consistent with 10 CFR 73.53(d)(2).
- Written implementing procedures will be established and maintained on site to document the measures taken to address the performance specifications associated with the identified cyber security controls, consistent with 10 CFR 73.53(d)(5)
- The cyber security program will include appropriate interim compensatory measures, configuration management, documentation, recordkeeping, and reporting to the NRC.
- Identification and documentation of digital assets and vital digital assets (VDAs) will be completed within 6 months of NRC approval of this Plan.
- Full implementation of this Plan will occur within 18 months of its approval by NRC.

CHAPTER 3 CYBER SECURITY TEAM

[DESCRIBE THE STRUCTURE OF THE CYBER SECURITY TEAM.]

3.1 STRUCTURE AND STAFFING

[IDENTIFY KEY POSITIONS BY TITLE INCLUDING CYBER SECURITY PROGRAM MANAGER (EXECUTIVE LEVEL), PROGRAM MANAGER, OPERATION SPECIALISTS, AND TECHNICAL STAFF. IF APPLICABLE, REFERENCE ONSITE DOCUMENTATION OF THE NAMES AND CONTACT INFORMATION FOR INDIVIDUALS FILLING KEY POSITIONS ON THE TEAM RATHER THAN INCORPORATING THEM IN THE PLAN.]

[DEFINE THE POSITION ROLES AND RESPONSIBILITIES.]

3.2 TRAINING AND QUALIFICATION

[DESCRIBE THE MINIMUM LEVEL OF TRAINING PROVIDED FOR EACH POSITION ON THE CST DEPENDING ON THE ROLES AND RESPONSIBILITIES OF THAT POSITION.]

[ESTABLISH AND DOCUMENT MINIMUM QUALIFICATION REQUIREMENTS FOR EACH KEY POSITION ON THE CST.]

3.3 EQUIPMENT

[DOCUMENT A COMMITMENT TO PROVIDE THE CYBER SECURITY TEAM (CST) WITH THE APPROPRIATE SOFTWARE, TOOLS, AND DEVICES TO VERIFY DIGITAL ASSETS ARE OPERATING WITHIN ACCEPTABLE PARAMETERS AND CAN CONDUCT THE PERIODIC AUDIT OF THE VDA DEFENSES.]

CHAPTER 4 CYBER SECURITY PROGRAM MANAGEMENT AND INCIDENT RESPONSE

4.1 MANAGING THE CYBER SECURITY PROGRAM

[DESCRIBE HOW THE CYBER SECURITY PROGRAM WILL BE MANAGED. PROVIDE THE GOALS FOR OPERATION AFTER THE PROGRAM IS FULLY IMPLEMENTED. DESCRIBE HOW THE CST AND ITS FUNCTIONS WILL CONTINUE TO SUPPORT THE CYBER SECURITY PROGRAM FOR THE LIFE OF THE FACILITY.]

[DESCRIBE HOW MANAGEMENT PRACTICES WILL BE ADJUSTED TO MAINTAIN THE EFFECTIVENESS OF THE CYBER SECURITY PROGRAM TO REFLECT THE RECOMMENDATIONS STEMMING FROM THE PERIODIC REVIEW.]

4.2 CYBER SECURITY INCIDENT RESPONSE

[INCORPORATE THE CYBER SECURITY INCIDENT RESPONSE PLAN (CSIRP) INTO THE CSP OR PROVIDE THE INFORMATION BY REFERENCE TO A SEPARATE CYBER SECURITY INCIDENT RESPONSE PLAN. IF A SEPARATE DOCUMENT IS USED, PROVIDE A SUFFICIENT COMMITMENT IN THE CSP TO MAKE THE CSIRP ENFORCEABLE.]

[DESCRIBE CYBER ATTACK DETECTION ACTIVITIES USED.]

[DESCRIBE THE CSIR MEASURES PLANNED FOR USE DURING A CYBER ATTACK TO A CYBER ATTACK AFFECTING VDAS OR THAT MAY CAUSE A CONSEQUENCE OF CONCERN.]

[DESCRIBE THE STRUCTURE OF THE CYBER SECURITY INCIDENT RESPONSE TEAM AND HOW IT IS ALLOCATED RECOURSES NECESSARY FOR RESPONSE AND STAFF ARE APPROPRIATELY TRAINED.]

[DESCRIBE HOW THE CAPACITY FOR INFORMATION PROCESSING, TELECOMMUNICATIONS, AND ENVIRONMENTAL SUPPORT IS MAINTAINED DURING THE CSIR. DESCRIBE HOW ESSENTIAL SAFETY AND SECURITY FUNCTIONS ARE MAINTAINED DURING A CSIR.]

[DESCRIBE HOW THE CSIR CAPABILITIES ARE TESTED AND THE FREQUENCY.]

CHAPTER 5 ADDRESSING CONSEQUENCES OF CONCERN

5.1 APPLICABLE TYPES OF CONSEQUENCES OF CONCERN

The cyber security program is designed to protect against the following types of consequences of concern:

[CATEGORY I FACILITIES ONLY –
Latent consequences of concern – design basis threat
The compromise, as a result of a cyber attack of a function needed to prevent one or more of the following:

- Radiological sabotage, as specified in 10 CFR 73.1(a)(1);
- Theft or diversion of formula quantities of strategic special nuclear material, as specified in 10 CFR 73.1(a)(2); or
- Loss of nuclear material control and accounting for strategic special nuclear material, as specified in 10 CFR 74.51(a).]

[CATEGORY II FACILITIES ONLY –
Latent consequences of concern – safeguards
The compromise, as a result of a cyber attack of a function needed to prevent one or more of the following:

- Unauthorized removal of special nuclear material of moderate strategic significance, as specified in 10 CFR 73.67(d); or
- Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance, as specified in 10 CFR 74.41(a).]

Active consequences of concern – safety
One or more of the following that directly results from a cyber attack:

- Radiological exposure of 25 rem or greater for any individual;
- 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or
- An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

Latent consequences of concern – safety and security
The compromise, as a result of a cyber attack, of a function needed to prevent:

- Radiological exposure of 25 rem or greater for any individual;
- 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area;
- An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual; or
- Loss or unauthorized disclosure of classified information or classified matter.

5.2 SITE SPECIFIC CONSIDERATIONS FOR THE APPLICABLE TYPES OF CONSEQUENCES OF CONCERN

[REFERENCE SITE SPECIFIC DOCUMENTATION THAT WILL BE USED TO CONSIDER THE POTENTIAL CONSEQUENCES OF CONCERN FROM A CYBER ATTACK (E.G., INTEGRATED SAFETY ANALYSIS, PROCESS HAZARDS ANALYSIS, PHYSICAL SECURITY PLAN, MATERIAL CONTROL AND ACCOUNTING PLAN, VULNERABILITY ANALYSIS)]

[DESCRIBE SITE SPECIFIC VALUES ASSOCIATED WITH THRESHOLDS FOR CONSEQUENCES OF CONCERN (E.G., LEVELS FOR ACUTE CHEMICAL EXPOSURE FROM INTEGRATED SAFETY ANALYSIS) THAT ARE USED TO INFORM THE IDENTIFICATION OF DIGITAL ASSETS THAT NEED TO BE PROTECTED FROM A CYBER ATTACK.]

CHAPTER 6 IDENTIFICATION OF DIGITAL ASSETS

6.1 IDENTIFYING DIGITAL ASSETS ASSOCIATED WITH A CONSEQUENCE OF CONCERN

[DESCRIBE THE PROCESS TO IDENTIFY DIGITAL ASSETS THAT, IF COMPROMISED BY A CYBER ATTACK, COULD RESULT IN A CONSEQUENCES OF CONCERN IN SUFFICIENT DETAIL FOR NRC TO DETERMINE THE APPROACH]

[DESCRIBE THE PROCESS USED TO CONFIRM THAT VDAS WITH THE POTENTIAL TO HAVE MULTIPLE CONSEQUENCES OF CONCERN HAVE THE APPROPRIATE CONTROLS APPLIED.]

[PROVIDE A COMMITMENT TO DOCUMENT DIGITAL ASSETS ASSOCIATED WITH A CONSEQUENCE OF CONCERN LISTING, AT A MINIMUM:

- THE NAME AND PHYSICAL LOCATION OF THE APPLICATION, DEVICE, SYSTEM, OR NETWORK IDENTIFIED AS A DIGITAL ASSET; AND
- WHICH TYPES OF CONSEQUENCES OF CONCERN ARE POTENTIALLY APPLICABLE IF A COMPROMISE OF THE DIGITAL ASSET WERE TO OCCUR.]

6.2 ALTERNATE MEANS ANALYSIS

[DESCRIBE THE PROCESS USED TO IDENTIFY ALTERNATE MEANS FOR DIGITAL ASSETS TO PREVENT A CONSEQUENCE OF CONCERN. DESCRIBE THE LEVEL OF VERIFICATION UNDERTAKEN TO ENSURE THE ALTERNATE MEANS REMAIN AVAILABLE, RELIABLE, AND PROTECTED FROM A CYBER ATTACK.]

6.3 VITAL DIGITAL ASSETS

[DESCRIBE HOW VDAS ARE DOCUMENTED IN THE IMPLEMENTING PROCEDURES.]

[PROVIDE A COMMITMENT FOR IMPLEMENTING PROCEDURES TO DOCUMENT, AT A MINIMUM, THE FOLLOWING:

- A GENERAL DESCRIPTION, INCLUDING THE PHYSICAL AND LOGICAL LOCATION, OF EACH APPLICATION, DEVICE, SYSTEM, OR NETWORK IDENTIFIED AS A VDA;
- A BRIEF DESCRIPTION OF THE FUNCTION(S) PROVIDED BY THE VDA, INCLUDING WHICH OF THE FOUR TYPES OF CONSEQUENCES OF CONCERN ARE APPLICABLE IF A COMPROMISE OF THE DIGITAL ASSET WERE TO OCCUR; AND
- IDENTIFICATION OF SUPPORT SYSTEMS FOR THE VDA THAT, IF COMPROMISED BY A CYBER ATTACK, WOULD CAUSE THE CONSEQUENCE(S) OF CONCERN.]

6.4 BOUNDARIES FOR VITAL DIGITAL ASSETS

[DESCRIBE THE CRITERIA USED TO DETERMINE THE BOUNDARY FOR VDAS. PROVIDE A COMMITMENT TO DOCUMENT THE BOUNDARY IN THE APPROPRIATE IMPLEMENTING PROCEDURE.]

6.5 SUPPORT SYSTEMS FOR VITAL DIGITAL ASSETS

[DESCRIBE HOW SUPPORT SYSTEMS ARE ANALYZED TO DETERMINE THE INTERDEPENDENCE BETWEEN THE SUPPORT SYSTEM AND THE VDA.]

[PROVIDE A COMMITMENT TO PROTECT SUPPORT SYSTEMS THAT COULD COMPROMISE A VDA AND RESULT IN A CONSEQUENCE OF CONCERN.]

[PROVIDE A COMMITMENT TO DOCUMENT SUPPORT SYSTEMS IN THE APPROPRIATE IMPLEMENTING PROCEDURE(S).]

6.6 GROUPING OF VITAL DIGITAL ASSETS

[DESCRIBE THE METHODOLOGY THE LICENSEE USES TO GROUP SIMILAR VDAS, WHEN APPROPRIATE.]

[PROVIDE A COMMITMENT TO, WHEN GROUPING OF VDAS IS USED, DOCUMENT THE JUSTIFICATION IN THE APPROPRIATE IMPLEMENTING PROCEDURE(S).]

CHAPTER 7 CYBER SECURITY CONTROLS

7.1 STANDARDS AND APPLICABLE CYBER SECURITY CONTROLS

[PROVIDE THE SOURCE FOR THE CYBER SECURITY CONTROLS USED TO PROTECT VDAS (E.G., NRC REGULATORY GUIDE, NIST STANDARDS, ISO STANDARDS)]

7.2 ESTABLISHING AND MAINTAINING CYBER SECURITY CONTROLS

[PROVIDE OR REFERENCE THE CYBER SECURITY CONTROLS, INCLUDING THEIR PERFORMANCE SPECIFICATIONS AND PARAMETER CONSIDERATIONS, SPECIFIC TO EACH TYPE OF CONSEQUENCE OF CONCERN LISTED IN CHAPTER 5 OF THIS PLAN.]

[DESCRIBE HOW CYBER SECURITY CONTROLS WILL BE MAINTAINED.]

7.3 TAILORING CYBER SECURITY CONTROLS FOR SPECIFIC VITAL DIGITAL ASSETS

[DESCRIBE THE PROCESS USED TO DETERMINE WHICH CYBER SECURITY CONTROLS ARE USED FOR A VDA.]

[DESCRIBE THE PROCESS USED TO TAILOR THE CYBER SECURITY CONTROLS AND DETERMINE THEIR PARAMETERS THAT ARE SPECIFIC TO THE VDA]

7.4 COMMON AND INHERITED CYBER SECURITY CONTROLS

[IF COMMON AND INHERITED CONTROLS WILL BE USED, DESCRIBE HOW THEY WILL BE IMPLEMENTED.]

7.5 VERIFYING CYBER SECURITY CONTROLS

[DESCRIBE THE PROCESS USED TO VERIFY THE CYBER SECURITY CONTROLS ASSOCIATED WITH A SPECIFIC VDA]

CHAPTER 8 IMPLEMENTING PROCEDURES AND INTERIM COMPENSATORY MEASURES

8.1 IMPLEMENTING PROCEDURES

[PROVIDE A COMMITMENT TO ESTABLISH AND MAINTAIN APPROPRIATE IMPLEMENTING PROCEDURES TO DOCUMENT MEASURES TAKEN TO MEET PERFORMANCE SPECIFICATIONS FOR CYBER SECURITY CONTROLS.]

8.2 INTERIM COMPENSATORY MEASURES

[PROVIDE A COMMITMENT TO USE INTERIM COMPENSATORY MEASURES (ICMS) WHEN AND WHERE NECESSARY.]

[DESCRIBE HOW THE ICMS ARE TRACKED AND VERIFIED TO ADDRESS ASSOCIATED CYBER SECURITY CONTROLS EFFECTIVELY.]

CHAPTER 9 CONFIGURATION MANAGEMENT

[DESCRIBE THE CONFIGURATION MANAGEMENT SYSTEM FOR CYBER SECURITY USED TO ANALYZE FACILITY CHANGES AND INCLUDE THE ROLES AND RESPONSIBILITIES.]

9.1 CYBER SECURITY IMPACT ANALYSIS

[DESCRIBE HOW THE CYBER SECURITY IMPACT ANALYSIS FOR CHANGES TO THE FACILITY WILL BE COMPLETED]

9.2 SITE-WIDE CONSIDERATIONS

[DESCRIBE THE VDA AUTHORIZATION PROCESS FOR THE FULLY IMPLEMENTED CYBER SECURITY PROGRAM.]

CHAPTER 10 REVIEW OF THE CYBER SECURITY PROGRAM

A review of the cyber security program will occur

[CATEGORY I FACILITIES ONLY – as a component of the security program in accordance with the requirements of §73.46(g)(6).]

[ALL OTHER FACILITIES – at least every 36 months.]

The review will include an audit of the effectiveness and adequacy of the cyber security program including, but not limited to:

- Implementing procedures; and
- Applicable cyber security controls, alternate means of protection, and defensive architecture for the digital assets identified through Chapter 6 of this Plan.

The findings, deficiencies, and recommendations resulting from the review will be:

- Tracked and addressed in a timely manner; and
- Documented in a report to the [INSERT NAME OR TITLE OF PLANT MANAGER] and to [INSERT NAME OR TITLE OF CORPORATE MANAGEMENT AT LEAST ONE LEVEL HIGHER THAN THAT HAVING RESPONSIBILITY FOR DAY-TO-DAY PLANT OPERATIONS].

[DESCRIBE SITE SPECIFIC PROCESSES USED TO REVIEW, EVALUATE, AND DOCUMENT THE EFFECTIVENESS AND ADEQUACY OF THE CYBER SECURITY PROGRAM.]

CHAPTER 11 EVENT REPORTING AND TRACKING

The NRC Headquarters Operations Center will be informed upon discovery that an event requiring notification under existing NRC regulations is the result of a cyber attack, as required by 10 CFR 73.53(h).

The following must be recorded, within 24 hours of discovery, and tracked to resolution:

- A failure, compromise, discovered vulnerability, or degradation that results in a decrease in effectiveness of a cyber security control protecting a vital digital asset.

[FOR CATEGORY I FACILITIES ONLY –

- A cyber attack that compromises a vital digital asset associated with the loss of nuclear material control and accounting for strategic special nuclear material, as specified in 10 CFR 74.51(a).]

[FOR CATEGORY II FACILITIES ONLY –

- A cyber attack that compromises a vital digital asset associated with the loss of nuclear material control and accounting for special nuclear material of moderate strategic significance, as specified in 10 CFR 74.41(a).]

[IDENTIFY THE LOGS USED FOR RECORDING RELEVANT EVENTS] will be used to record 24 hour cyber security events.

CHAPTER 12 RECORDKEEPING

Supporting technical documentation demonstrating compliance with the requirements of 10 CFR 73.53 will be retained as a record. All records, reports, and documents required to be kept by Commission regulations, orders, or license conditions will be maintained and made available for inspection until the NRC terminates the license. Superseded portions of these records, reports, and documents will be maintained for at least 3 years after they are superseded, unless otherwise specified by the NRC.

[DESCRIBE SITE SPECIFIC RECORDKEEPING.]

APPENDIX B

CYBER SECURITY CONTROLS FOR VITAL DIGITAL ASSETS ASSOCIATED WITH ANY CONSEQUENCE OF CONCERN

B-1 DETECTION

(Informed by National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cyber Security)

[Licensee/Applicant]:

- Monitors the effectiveness of the measures used to protect those assets from a cyber attack; and
- Takes the following actions to detect potential cyber attacks:
    - Monitor networks associated with a vital digital asset (VDA);
    - Monitor the physical environment in conjunction with the physical security program;
    - Monitor activity within VDAs;
    - Monitor external service provider or contractor activity;
    - Scan for malicious or unauthorized code;
    - Perform vulnerability scans on the VDAs; and
    - Update vulnerability information regarding VDAs at least every 7 days.

B-2 POLICIES AND PROCEDURES

(Informed by NIST Special Publication (SP) 800-53, Rev. 4)

[Licensee/Applicant] develops, documents, and disseminates to all personnel, including contractors, the following policies and procedures:

- Access Control;
- Security awareness and training;
- Audit and accountability;
- System and Information integrity;
- Identification and authentication;
- System maintenance;
- Media protection;
- System and services acquisition; and
- System and communications protection.

These policies and procedures will:

- Address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Facilitate the implementation of the policy and associated security controls; and
- Are reviewed and updated at least every 24 months, when changes occur in VDAs, the environment that may adversely impact the cyber security program, or the licensee's ability to prevent a consequence of concern.

B-3 SEPARATION OF DUTIES
(Informed by NIST SP 800-53 Rev. 4, AC-5)

[Licensee/Applicant]:

- Separates the duties of VDA management, programming, configuration management, quality assurance and testing, and network security for VDAs;
- Documents the separation of duties of individuals; and
- Defines access authorizations to support separation of duties.

B-4 LEAST PRIVILEGE
(Informed by NIST SP 800-53 Rev. 4, AC-6)

[Licensee/Applicant] employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks when it is not technically feasible to perform the function with a non-privileged account.

B-5 AUTHORIZE ACCESS TO SECURITY FUNCTIONS
(Informed by NIST SP 800-53 Rev. 4, AC-6 (1))

[Licensee/Applicant] explicitly authorizes access to VDAs, and security functions credited with protected VDAs (deployed in hardware, software, and firmware) and security-relevant information.

B-6 NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS
(Informed by NIST SP 800-53 Rev. 4, AC-6 (2))

[Licensee/Applicant] requires that users of accounts or roles with access to VDAs, security functions credited with protecting a VDA, or security-relevant information use non-privileged accounts or roles when accessing nonsecurity functions.

B-7 NETWORK ACCESS TO PRIVILEGED COMMANDS
(Informed by NIST SP 800-53 Rev. 4, AC-6 (3))

[Licensee/Applicant] authorizes network access to privileged commands only for compelling operational needs and documents the rationale for such access.

B-8 PRIVILEGED ACCOUNTS
(Informed by NIST SP 800-53 Rev. 4, AC-6 (5))

[Licensee/Applicant] restricts privileged accounts on the VDA to personnel or roles that, due to the design of the VDA, must have this access and implements adequate protection to ensure this access is monitored and unauthorized access is prohibited.

B-9 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, AC-14)

[Licensee/Applicant] identifies and documents user actions that can be performed on the VDA without identification or authentication, and documents supporting rationale for user actions not requiring identification or authentication.

B-10 PRIVILEGED COMMANDS AND ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-17 (4))

[Licensee/Applicant]:

- Authorizes the execution of privileged commands and access to security-relevant information via remote access only for the necessary, safe operation of the VDA or to prevent a consequence of concern; and
- Documents the rationale for such access in the security plan for the VDA.

B-11 ACCESS CONTROL FOR MOBILE DEVICES
(Informed by NIST SP 800-53 Rev. 4, AC-19)

[Licensee/Applicant]:

- Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for mobile devices; and
- Authorizes the connection of mobile devices to organizational VDAs.

B-12 FULL-DEVICE OR CONTAINER-BASED ENCRYPTION
(Informed by NIST SP 800-53 Rev. 4, AC-19 (5))

[Licensee/Applicant] employs full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices used with VDAs.

B-13 PUBLICLY ACCESSIBLE CONTENT
(Informed by NIST SP 800-53 Rev. 4, AC-22)

[Licensee/Applicant]:

- Designates individuals authorized to post information onto a publicly accessible VDA;
- Trains authorized individuals to ensure that publicly accessible information does not contain security sensitive information;
- Reviews the proposed content of information prior to posting onto the publicly accessible VDA to ensure that nonpublic information is not included; and
- Reviews the content on the publicly accessible VDA for nonpublic information at least every 30 days and removes such information, if discovered.

B-14 LOG EVENTS
(Informed by NIST SP 800-53 Rev. 4, AU-2)

[Licensee/Applicant]:

- Develops and documents a list of auditable records that provide adequate information to prevent a consequence of concern including, at a minimum, the following events: user login or logouts; configuration, software, or firmware changes; audit setting changes; privileged access or commands; and any modifications of the security functions of VDAs;
- Determines that the VDA is capable of generating auditable records which can be reviewed in a timely manner;
- Coordinates the security audit function internally with personnel and groups requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
- Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

B-15 REVIEWS AND UPDATES
(Informed by NIST SP 800-53 Rev. 4, AU-2 (3))

[Licensee/Applicant] reviews and updates the list of auditable records at least every 12 months or based on current threat intelligence information, detection mechanisms, and configuration management activities, whichever is more frequently.

B-16 AUDIT RECORD RETENTION
(Informed by NIST SP 800-53 Rev. 4, AU-11)

[Licensee/Applicant] retains audit records until the record is superseded to provide support for after-the-fact investigations of security incidents and to meet U.S. Nuclear Regulatory Commission (NRC) record retention requirements.

B-17 VDA CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-3**)**

[Licensee/Applicant]:

- Authorizes connections from the VDA to other digital assets;
- Documents for each interconnection the interface characteristics, security requirements, and the nature of the information communicated; and
- Reviews and updates the authorizations at least every 12 months.

B-18 CONTINUOUS MONITORING
(Informed by NIST SP 800-53 Rev. 4, CA-7)

[Licensee/Applicant] develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

- Establishment and monitoring of sufficient cyber security metrics to provide adequate confirmation that security controls are in place and effective;
- Establishment, justification, and documentation of the monitoring and assessment frequencies for each metric;
- Ongoing security control assessments in accordance with the continuous monitoring strategy;
- Ongoing security status monitoring of cyber security metrics in accordance with the continuous monitoring strategy;
- Correlation and analysis of security-related information generated by assessments and monitoring;
- Response actions to address results of the analysis of security-related information; and
- Documenting the security status of the VDAs and their operating environment by the Cyber Security Team (CST) at least every 30 days.

B-19 BASELINE CONFIGURATION
(Informed by NIST SP 800-53 Rev. 4, CM-2 and CM-2 (1))

[Licensee/Applicant]:

- Develops, documents, and maintains under configuration control, a current baseline configuration of the VDA;
- Reviews the baseline configuration of the VDA when required due to an identified vulnerability, relevant change in threat intelligence, or suspected compromise; and

- Updates the baseline configuration of the VDA as an integral part of modifications.

B-20 AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES
(Informed by NIST SP 800-53 Rev. 4, CM-3 (1))

[Licensee/Applicant] employs automated mechanisms to:

- Document proposed changes to the VDA;
- Notify appropriate personnel of proposed changes to the VDA and request change approval;
- Prohibit changes to the VDA until designated approvals are received;
- Document all changes to the VDA; and
- Notify appropriate personnel when approved changes to the VDA are completed.

B-21 ACCESS CONTROL FOR TRANSMISSION MEDIUM
(Informed by NIST SP 800-53 Rev. 4, PE-4)

[Licensee/Applicant] controls physical access to VDA distribution and transmission lines such that they are adequately protected to prevent a consequence of concern.

B-22 ACCESS CONTROL FOR OUTPUT DEVICES
(Informed by NIST SP 800-53 Rev. 4, PE-5)

[Licensee/Applicant] controls physical access to VDA output devices to prevent unauthorized individuals from obtaining the output.

B-23 IMPLEMENTING PROCEDURES FOR VDAS
(Informed by NIST SP 800-53 Rev. 4, PL-2 and PL-2 (3))

[Licensee/Applicant]:

- Develops implementing procedures for each VDA that:
    - Provides the associated consequence of concern for the VDA including supporting rationale;
    - Describes the operational environment for the VDA and relationships with or connections to other digital assets;
    - Provides an overview of the security requirements for the VDA;
    - Describes the cyber security measures in place or planned for meeting cyber security control requirements including a rationale for equivalent measures; and
- Distributes copies of the implementing procedures and communicates subsequent changes to the procedures only to authorized personnel with a need-to-know;
- Updates the procedures to address changes to the VDA and environment of operation or problems identified during the performance of implementing procedures or security control assessments;
- Protects the implementing procedures from unauthorized disclosure and modification; and
- Plans and coordinates security-related activities affecting the VDA with the CST before conducting such activities in order to reduce the impact on other organizational entities.

B-24 CYBER SECURITY ARCHITECTURE
(Informed by NIST SP 800-53 Rev. 4, PL-8 and PL-8 (1))

[Licensee/Applicant]:

- Documents an cyber security architecture for the VDA that:

  - Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of VDA or related information;
  - Describes any security assumptions about, and dependencies on, external services; and
- Reviews and updates the cyber security architecture at least every 24 months to reflect updates; and
- Ensures that planned cyber security architecture changes are reflected in the implementing procedures, procurements, and acquisitions.

[Licensee/Applicant] designs its security architecture using a defense-in-depth approach that:

- Employs complementary and redundant cyber security measures that establish multiple layers of protection to safeguard VDAs;
- Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner; and
- Ensures the capability to detect, prevent, respond to, and mitigate cyber attacks.

B-25 ACQUISITION PROCESS
(Informed by NIST SP 800-53 Rev. 4, SA-4)

[Licensee/Applicant] includes explicitly or by reference the following requirements, descriptions, and criteria in the acquisition contract for the VDA, its components, or related services:

- Security functional requirements;
- Security strength requirements;
- Security assurance requirements;
- Security-related documentation requirements;
- Requirements for protecting security-related documentation;
- Description of the VDA development environment and environment in which the VDA is intended to operate; and
- Acceptance criteria.

B-26 FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
(Informed by NIST SP 800-53 Rev. 4, SA-4, SA-4 (1), SA-4 (2), and SA-4 (9))

[Licensee/Applicant] requires the developer of the VDA, component, or service to:

- Provide a description of the functional security properties, design, and implementation information to be employed, with sufficient documentation to support the licensee's conclusions that the functional security features will work as intended; and
- Identify the functions, ports, protocols, and services employed.

B-27 NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)–APPROVED PROTECTION PROFILES
(Informed by NIST SP 800-53 Rev. 4, SA-4 (7))

[Licensee/Applicant]:

- Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a NIAP-approved Protection Profile for a specific technology type, if such a profile exists; and
- Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is validated by the NIST Cryptographic Module Validation Program.

B-28 USE OF APPROVED PIV PRODUCTS
(Informed by NIST SP 800-53 Rev. 4, SA-4 (10))

[Licensee/Applicant] employs only technology on the Federal Information Processing Standard 201-approved products list for Personal Identity Verification capabilities used to protect VDAs.

B-29 VDA DOCUMENTATION
(Informed by NIST SP 800-53 Rev. 4, SA-5)

[Licensee/Applicant]:

- Obtains administrator documentation for the VDA, component, or service that describes:
  - Secure configuration, installation, and operation;
  - Effective use and maintenance of security functions and mechanisms;
  - Known vulnerabilities regarding configuration and use of administrative and privileged functions; and
- Obtains user documentation for the VDA, component, or service that describes:
  - User-accessible security functions and mechanisms and how to effectively use those security functions and mechanisms;
  - Methods for user interaction, which enables individuals to use the VDA, component, or service in a more secure manner;
  - User responsibilities in maintaining the security of the VDA, component, or service; and
- Documents the attempts to obtain VDA, component, or service documentation when such documentation is either unavailable or nonexistent and take appropriate actions to compensate for the lack of information regarding the security features;
- Protects documentation from unauthorized access; and
- Distributes documentation to authorized personnel on a need-to-know basis.

B-30 SECURITY ENGINEERING PRINCIPLES
(Informed by NIST SP 800-53 Rev. 4, SA-8)

[Licensee/Applicant] applies cyber security engineering principles in the specification, design, development, implementation, and modification of the VDA.

B-31 DEVELOPER-PROVIDED TRAINING
(Informed by NIST SP 800-53 Rev. 4, SA-16)

[Licensee/Applicant] requires the developer of the VDA, component, or service to provide adequate role-based training on the correct use and operation of the implemented security functions, controls, and mechanisms.

B-32 MOBILE CODE
(Informed by NIST SP 800-53 Rev. 4, SC-18)

[Licensee/Applicant]:

- Defines a technical basis for acceptable and unacceptable mobile code and mobile code technologies to prevent a consequence of concern;
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- Authorizes, monitors, and controls the use of mobile code within the VDA.

B-33 INFORMATION INPUT VALIDATION
(Informed by NIST SP 800-53 Rev. 4, SI-10)

[Licensee/Applicant]:

- Ensures the VDA checks the validity of information inputs automatically for accuracy, completeness, validity, and authenticity;
- Enforces that rules for checking the valid syntax of VDA inputs (e.g., character set, length, numerical range, acceptable values) are documented and in place to verify that inputs match specified definitions for format and content; and
- Confirms that inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

B-34 CONFIGURATION MANAGEMENT PLAN
(Informed by NIST SP 800-53 Rev. 4, CM-1)

[Licensee/Applicant] develops, documents, and implements a configuration management plan for the VDA that:

- Addresses roles, responsibilities, and configuration management processes and procedures;
- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
- Defines the configuration items for the VDA and places the configuration items under configuration management; and
- Protects the configuration management plan from unauthorized disclosure and modification.

B-35 SECURITY AWARENESS TRAINING
(Informed by NIST SP 800-53 Rev. 4, AT-1)

[Licensee/Applicant]:

- Provides basic security awareness training to VDA users (including managers, senior executives, and contractors):
  - As part of initial training for new users;
  - When required by VDA changes;
  - At least every 12 months thereafter; and
- Provides role-based security training to personnel with assigned security roles and responsibilities:
  - Before authorizing access to the VDA or performing assigned duties;
  - When required by VDA changes;
  - At least every 12 months thereafter; and
- Documents and monitors individual VDA security training activities including basic security awareness training and specific VDA security training; and
- Retains individual training records consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53(i).

B-36 PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

(Informed by NIST SP 800-53 Rev. 4, AC-6 (10))

[Licensee/Applicant] ensures the VDA prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards and measures.

B-37 UNSUCCESSFUL LOGON ATTEMPTS

(Informed by NIST SP 800-53 Rev. 4, AC-7)

[Licensee/Applicant]:

- Limits the number of failed login attempts in a specified time period, which may vary by VDA (i.e., more than three invalid attempts within a 1-hour time period will automatically lock out the account); and
- Ensures the VDA enforces the lock out mode automatically.

B-38 PURGE OR WIPE MOBILE DEVICE

(Informed by NIST SP 800-53 Rev. 4, AC-7 (2))

[Licensee/Applicant] ensures that, for mobile devices used with VDAs, the mobile device purges or wipes information in a manner that would prevent recovery of the data by an adversary within 10 consecutive unsuccessful device logon attempts.

B-39 VDA USE NOTIFICATION

(Informed by NIST SP 800-53 Rev. 4, AC-8)

[Licensee/Applicant] ensures VDAs display to users a use notification message or banner before granting access that provides appropriate security notices consistent with NRC regulations, and to support the prevention of consequence of concern, and retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the VDA. The notice informs the user that:

- Users are accessing a VDA;
- Usage may be monitored, recorded, and subject to audit;
- Unauthorized use is prohibited and subject to criminal and civil penalties;
- Use indicates consent to monitoring and recording; and
- For publicly accessible VDAs:
  - Displays VDA use information before granting further access;
  - Displays references, if any, to monitoring, recording, or auditing that are consistent with the requirements for non-public VDAs; and
  - Includes a description of the authorized uses.

B-40 CONCURRENT SESSION CONTROL

(Informed by NIST SP 800-53 Rev. 4, AC-10)

[Licensee/Applicant] ensures the VDA limits the number of concurrent sessions for each account and account type to the minimum necessary to perform the VDA's function.

B-41 SESSION LOCK AND TERMINATION
(Informed by NIST SP 800-53 Rev. 4, AC-11 and AC-12)

[Licensee/Applicant] ensures the VDA:

- Prevents further access to, and conceals information previously visible on, the display by initiating a session lock within 30 minutes of inactivity or upon receiving a request from a user;
- Retains the session lock until the user reestablishes access using established identification and authentication procedures; and
- Automatically terminates a user session within 45 minutes of inactivity.

B-42 AUTOMATED MONITORING / CONTROL
(Informed by NIST SP 800-53 Rev. 4, AC-17 (1))

[Licensee/Applicant] ensures the VDA monitors and controls remote access methods.

B-43 PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION
(Informed by NIST SP 800-53 Rev. 4, AC-17 (2))

[Licensee/Applicant] ensures the VDA implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

B-44 AUTHENTICATION AND ENCRYPTION
(Informed by NIST SP 800-53 Rev. 4, AC-18 (1))

[Licensee/Applicant] ensures the VDA protects wireless access to the VDA using authentication of users and encryption.

B-45 LOG REDUCTION AND REPORT GENERATION
(Informed by NIST SP 800-53 Rev. 4, AU-7)

[Licensee/Applicant] ensures the VDA provides a log reduction and report generation capability that:

- Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
- Does not alter the original content or time ordering of audit records.

B-46 AUTOMATIC PROCESSING
(Informed by NIST SP 800-53 Rev. 4, AU-7 (1))

[Licensee/Applicant] ensures the VDA provides the capability to process audit event and log records based on events of interest identified by the content of the specific audit record.

B-47 TIME STAMPS
(Informed by NIST SP 800-53 Rev. 4, AU-8)

[Licensee/Applicant]:

- Uses a time source protected at an equal or greater level than the VDAs they support; and
- Ensures the VDA:

- Implements time synchronization mechanisms that do not introduce a vulnerability leading to a consequence of concern;
- Synchronizes its internal clock from the protected time source; and
- Uses its internal clock to generate time stamps for audit records.

B-48 SUPPLY CHAIN PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SA-12)

[Licensee/Applicant] protects against supply chain threats to the VDA, component, or information system service by:

- Establishing of trusted distribution paths;
- Validating vendors; and
- Requiring tamper proof products or tamper evident seals on acquired products as part of a comprehensive, defense-in-breadth information security strategy.

APPENDIX C

ADDITIONAL CYBER SECURITY CONTROLS FOR VITAL DIGITAL ASSETS ASSOCIATED WITH LATENT CONSEQUENCES OF CONCERN – DESIGN BASIS THREAT (CATEGORY I FACILITIES ONLY)

C-1 INSIDER THREAT PROGRAM

(Informed by National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, PM-12 and AT-2 (2))

[Licensee/Applicant] implements an insider threat program that includes a cross-discipline insider threat incident handling team. [Licensee/Applicant] includes security awareness training on recognizing and reporting potential indicators of insider threat.

C-2 ACCOUNT MANAGEMENT PROCEDURES

(Informed by NIST SP 800-53 Rev. 4, AC-2)

[Licensee/Applicant] employs, at a minimum, the following measures in support of the management of user accounts on vital digital assets (VDAs):

- Assigns account managers for VDA accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires independent management approval for requests to create VDA accounts;
- Creates, enables, modifies, disables, and removes VDA accounts in accordance with the Access Control policy;
- Monitors the use of VDA accounts;
- Notifies account managers in a timely manner:
  - When accounts are no longer required;
  - When users are terminated or transferred;
  - When individual VDA usage or need-to-know changes; and
- Authorizes access to the VDA based on:
  - A valid access authorization;
  - Intended VDA usage; and
- Reviews accounts at least every 30 days for compliance with account management requirements; and
- Employs, at a minimum, the following measures to restrict the creation and issuance of shared/group VDA accounts:
  - Ensures shared/group account requests:
    - Are issued only when necessary to prevent a consequence of concern;
    - Include a documented technical justification;
    - Are reviewed and approved by the Cyber Security Team (CST) prior to issuance; and
  - Automatically terminates and establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

C-3 ACCOUNT MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-2(5), AC-2(12), and AC-2(13))

[Licensee/Applicant] employs, at minimum, the following measures in support of the management of VDA accounts using a combination of procedural activity and automated means:

- Requires that users log out within 15 minutes of inactivity unless the login session must be maintained to prevent a consequence of concern;
- Monitors VDA accounts for atypical usage and anomalous activity that could indicate account compromise;
- Reports atypical usage of VDA accounts to the CST; and
- Disables user accounts that have been potentially compromised upon discovery.

C-4 AUTOMATED ACCOUNT MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-2 (1), AC-2 (2), AC-2 (3), AC-2 (4) and AC-2 (11))

[Licensee/Applicant] employs, at minimum, the following automated technical mechanisms to support the management of VDA accounts, including:

- Automatically removes or disables temporary and emergency accounts once they are no longer needed;
- Automatically disables inactive accounts within 30 days; and
- Automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate personnel in a timely manner.

C-5 ACCESS MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-3, AC-3 (2), AC-4, AC-4 (4), and AC-4 (21))

[Licensee/Applicant] ensures the VDA employs technical measures in support of the enforcement of account access to enforce approved authorizations for:

- Logical access to VDA information and VDA resources in accordance with applicable access control policies; and
- Controlling the flow of information within the VDA and between interconnected systems and VDAs.

[Licensee/Applicant] ensures the VDA employs automated technical measures to:

- Enforce dual authorization for privileged commands, operations or access;
- Prevent encrypted information from bypassing content-checking mechanisms;
- Separate information flows logically or physically; and
- Notify the user, upon successful logon/access:
  - The date and time of the last logon/access;
  - The number of unsuccessful logon/access attempts since the last successful logon/access;
  - The number of successful and unsuccessful logons/accesses within the last 7 days; and
  - Changes to security-related characteristics/parameters of the user's account within the last 7 days.

C-6 SECURITY ATTRIBUTES
(Informed by NIST SP 800-53 Rev. 4, AC-16, AC-16 (4), SC-16, and SC-16 (1))

[Licensee/Applicant]:

- Provides the means to associate security attributes with information in storage, in process, and/or in transmission;

- Ensures that the security attribute associations are made and retained with the information;
- Establishes the permitted security attributes for VDAs;
- Determines the permitted values or ranges for each of the established security attributes;
- Supports the association of security attributes for the VDA with information exchanged or transmitted between digital assets, VDAs, and components; and
- Validates the integrity of transmitted security attributes for the VDA.

C-7 MANAGED ACCESS CONTROL POINTS
(Informed by NIST SP 800-53 Rev. 4, AC-17 (3))

[Licensee/Applicant] prohibits all remote and off-site access to VDAs. Access to VDAs must be from a digital asset that is protected equivalent to the VDA.

C-8 USE OF EXTERNAL INFORMATION SYSTEMS
(Informed by NIST SP 800-53 Rev. 4, AC-20 (3), and AC-20 (4))

[Licensee/Applicant]:

- Prohibits the use of non-licensee owned information systems, VDA components, or devices used with VDAs; and
- Prohibits the use of organization-controlled network accessible storage devices] in external information systems.

C-9 CYBER SECURITY TRAINING
(Informed by NIST SP 800-53 Rev. 4, AT-2 (1) and AT-3 (3))

[Licensee/Applicant] includes practical exercises in security awareness training that simulate actual cyber attacks. [Licensee/Applicant] includes practical exercises in role based security training that reinforce training objectives.

[Licensee/Applicant] provides role based training to its personnel to recognize suspicious communications and anomalous behavior in VDAs.

C-10 AUDIT DATA DEFINITION, GENERATION, AND CONTENT
(Informed by NIST SP 800-53 Rev. 4, AU-3, AU-3 (1), AU-3 (2), AU-5, AU-5 (2), AU-12 (3), AU-14, AU-14 (1), and AU-14 (2))

[Licensee/Applicant] ensures the VDA:

- Generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event;
- Generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum:
  - Account (user or service) login failure and success;
  - Account role or privilege change;
  - File or object creation, modification and deletion;
  - Service start and stop;
  - Privileged service call;
  - Account creation, modification and deletion;
  - Account right assignment and removal;
  - Audit policy change;

- User account password change;
- User group creation, modification and deletion; and
- Remote session start, stop and failure.

[Licensee/Applicant] ensures the VDA auditing function:

- Alerts cyber security personnel in near real-time of an audit processing failure, or where audit failure events occur that could indicate VDA compromise;
- Takes automated measures to preserve audit data;
- Provides the capability to increase or modify audit record content in response to threat intelligence;
- Initiates session audits at VDA start-up;
- Provides the capability for authorized users to select a user session to capture/record or view/hear;
- Provides the capability for authorized users to capture/record and log content related to a user session; and
- Provides centralized management and configuration of the content to be captured in audit records.

C-11 AUDIT DATA MANAGEMENT AND PROTECTION
(Informed by NIST SP 800-53 Rev. 4, AU-4, AU-5 (1), AU-6 (7), AU-9, AU-9 (2), AU-9 (3), AU-9 (4), AU-9 (5), and AU-10)

[Licensee/Applicant]:

- Allocates sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configures auditing to prevent capacity from being exceeded;
- Authorizes access to management of audit functionality to only authorized users with cyber security responsibilities;
- Enforces dual authorization for movement or deletion of audit information;
- Specifies the permitted actions for each role or user associated with the review, analysis, and reporting of audit information;
- Ensures the VDA provides an alert to authorized personnel when allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity;
- Ensures the VDA backs up audit records onto a physically different VDA than the VDA being audited;
- Ensures the VDA protects audit information and audit tools from unauthorized access, modification, and deletion;
- Ensures the VDA implements cryptographic mechanisms to protect the integrity of audit information and audit tools; and
- Ensures the VDA protects against an individual (or process acting on behalf of an individual) falsely denying having performed any action on the VDA.

C-12 AUDIT REVIEW, ANALYSIS, AND REPORTING
(Informed by NIST SP 800-53 Rev. 4, AU-6, AU-6a, AU-6b, AU-6 (1), AU-6 (3), AU-6 (5), AU-6 (6), AU-10 (3), AU-10 (4), and AU-12 (1))

[Licensee/Applicant]:

- Employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities;
- Reviews and analyzes VDA audit records in a timely manner for indications of potential compromise;

- Analyzes and correlates audit records across different repositories to gain organization-wide situational awareness;
- Integrates analysis of audit records with analysis of vulnerability scanning information, performance data, VDA monitoring information, and data/information collected from other sources to further enhance the ability to identify potential unauthorized activity;
- Correlates information from audit records with information obtained from monitoring physical access to the VDA to further enhance the ability to identify potential unauthorized activity;
- Reports findings to the CST; and
- Ensures the VDA compiles audit records into a logical or physical audit trail that is time-correlated to, at a minimum, within one-tenth of a second.

[Licensee/Applicant] ensures the VDA:

- Maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released;
- Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer; and
- Prevents access to, modification of, or transfer of the information in the event of a validation error.

C-13 SECURITY CONTROL ASSESSMENTS

(Informed by NIST SP 800-53 Rev. 4, CA-2)

[Licensee/Applicant]:

- Develops a security assessment plan that describes the scope of the assessment including:
  - Security controls and control enhancements under assessment;
  - Assessment procedures to be used to determine security control effectiveness;
  - Assessment environment, assessment team, and assessment roles and responsibilities; and
- Assesses the security controls in the VDA and its environment of operation at least every 92 days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
- Produces a security assessment report that documents the results of the assessment;
- Includes and documents as part of VDA security control assessments:
  - An attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
  - Announced assessments:
    - In-depth monitoring (to be done automatically, in real time);
    - Vulnerability scanning (to be done at least every 30 days);
    - Malicious actor testing (to be done at least every 92 days);
    - Insider threat assessment (to be done at least every 92 days); and
  - Unannounced assessments (in addition to announced assessments above):
    - Vulnerability scanning (to be done at least every 183 days);
    - Malicious actor testing (to be done at least every 12 months);
    - Insider threat assessment (to be done at least every 183 days);
    - Performance/load testing (to be done at least every 183 days); and
  - Provides the results of the security control assessment to the CST; and
- Restricts access to the results of the security control assessment to authorized personnel with a need-to-know.

C-14 INDEPENDENCE OF ASSESSORS
(Informed by NIST SP 800-53 Rev. 4, CA-2 (1), CA-7 (1), CA-8, CA-8 (1), CA-8 (2))

[Licensee/Applicant]:

- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to conduct assessments of the cyber security controls;
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to monitor the cyber security controls for the VDA on an ongoing basis;
- Conducts penetration testing at least every 183 days on the VDA;
- Employs red team exercises to simulate attempts by adversaries to compromise VDAs; and
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to perform penetration testing on the VDA.

C-15 ENHANCEMENTS TO VDA CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant]:

- Employs a "deny-all, permit-by-exception" policy for allowing VDAs to connect to other digital assets;
- Prohibits access from and the connection of a VDA to an external network;
- Prohibits the direct connection of a VDA to a public network;
- Authorizes connections to the VDA; and
- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

C-16 NATIONAL SECURITY SYSTEM CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-3 (1))

For VDAs within NRC's regulatory purview store, process or transmit classified information or that qualify as a national security system, as defined by the Committee for National Security Systems, the licensee prohibits connection of the VDA to a public or external network.

C-17 INTERIM COMPENSATORY MEASURES
(Informed by NIST SP 800-53 Rev. 4, CA-5)

[Licensee/Applicant]:

- Documents an interim compensatory measure plan to correct weaknesses or deficiencies noted during the assessment of VDA security controls and to reduce or eliminate known vulnerabilities in the VDA;
- Updates interim compensatory measure plan at least every 30 days based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities; and
- Restricts access to the interim compensatory measure plan to authorized personnel with a need-to-know.

C-18 INTERNAL SYSTEM CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-9)

[Licensee/Applicant]:

- Authorizes internal connections of VDA components to the VDA; and
- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

C-19 AUTOMATED BASELINE CONFIGURATION
(Informed by NIST SP 800-53 Rev. 4, CM-2 (2))

[Licensee/Applicant] employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the VDA.

C-20 CONFIGURE VDAS FOR HIGH-RISK AREAS
(Informed by NIST SP 800-53 Rev. 4, CM-2 (7))

Prior to transporting VDAs associated with a design basis threat consequence of concern to locations that the [Licensee/Applicant] deems to be of significant risk, the [Licensee/Applicant]:

- Documents a detailed justification for the VDA to be transported;
- Obtains written approval from the CST and management;
- Documents the VDA configuration baseline and component inventory prior to leaving controlled areas;
- Ensures safeguards or security-related information on the VDA is purged or protected in a manner that prevents an adversary from recovering the data prior to leaving controlled areas;
- Observes chain-of-custody of the VDA or VDA component;
- Performs a review of the VDA configuration baseline and component inventory upon return;
- Performs testing of the VDA to ensure no cyber compromise has occurred; and
- Performs a security control assessment to ensure all controls are in place, operational, and performing the intended function.

C-21 CONFIGURATION CHANGE CONTROL
(Informed by NIST SP 800-53 Rev. 4, CM-3)

[Licensee/Applicant]:

- Documents changes to the VDA that will be configuration-controlled per Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53;
- Reviews proposed configuration-controlled changes to the VDA and approves or disapproves such changes with explicit consideration for security impact analyses before implementation of the change;
- Documents configuration change decisions associated with the VDA;
- Implements approved configuration-controlled changes to the VDA;
- Retains records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements;
- Audits and reviews activities associated with configuration-controlled changes to the VDA; and
- Coordinates and provides oversight for configuration change control activities through the change management process.

C-22 CHANGE TESTING AND ANALYSIS
(Informed by NIST SP 800-53 Rev. 4, CM-3 (2), CM-4, CM-4 (1), and CM-4 (2))

[Licensee/Applicant]:

- Tests, validates, and documents changes to the VDA before implementing the changes on the VDA;
- Analyzes changes to the VDA to determine potential security impacts prior to change implementation;
- Analyzes changes to the VDA in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; and
- Checks the security functions after a VDA is changed to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the VDA.

C-23 ACCESS RESTRICTIONS FOR CHANGE
(Informed by NIST SP 800-53 Rev. 4, CM-5, CM-5 (1), and CM-5 (4))

[Licensee/Applicant]:

- Defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the VDA;
- Enforces dual authorization for implementing changes to VDAs and components; and
- Enforces VDA access restrictions and supports auditing of the enforcement actions.

C-24 REVIEW VDA CHANGES
(Informed by NIST SP 800-53 Rev. 4, CM-5 (2))

[Licensee/Applicant] reviews VDA changes at least every 183 days or in the event of suspected compromise to determine whether unauthorized changes have occurred.

C-25 SIGNED COMPONENTS
(Informed by NIST SP 800-53 Rev. 4, CM-5 (3))

[Licensee/Applicant] ensures the VDA prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

C-26 CONFIGURATION SETTINGS
(Informed by NIST SP 800-53 Rev. 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant]:

- Establishes and documents configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves any deviations from established configuration settings;
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;
- Employs automated mechanisms to centrally manage, apply, and verify VDA configuration settings; and

- Reports unauthorized changes to VDA configuration settings to the cyber security incident response team upon detection.

C-27 LEAST FUNCTIONALITY
(Informed by NIST SP 800-53 Rev. 4, CM-7)

[Licensee/Applicant]:
- Configures the VDA to provide only essential capabilities, to perform its function and maintain safe and secure operations; and
- Prohibits or restricts the use of unneeded functions, ports, protocols, and/or services.

C-28 PERIODIC REVIEW
(Informed by NIST SP 800-53 Rev. 4, CM-7 (1))

[Licensee/Applicant]:
- Reviews the VDA continuously to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
- Disables or restricts unneeded functions, ports, protocols, and/or services identified by the review.

C-29 AUTHORIZED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-7 (2) CM-7 (5), CM-8 (1), CM-8 (2), and CM-8 (3))

[Licensee/Applicant]:
- Identifies software programs authorized to execute on the VDA;
- Employs an "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA;
- Reviews and updates the list of authorized software programs, at least every 92 days;
- Employs automated mechanisms for the VDA (i.e. application white-listing) to prevent unauthorized program execution;
- Develops and documents an inventory of information VDA components that:
  - Accurately reflects the current VDA;
  - Includes all components within the boundary of the VDA;
  - Is at the level of granularity necessary for tracking and reporting;
  - Includes information necessary to achieve effective information VDA component accountability; and
- Reviews and updates the VDA component inventory at least every 92 days or as part of any changes to a VDA;
- Updates the inventory of information VDA components as an integral part of component installations, removals, and VDA updates;
- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA;
- employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components; and
- Takes appropriate actions when unauthorized components are detected to remove, disable, or otherwise prevent the unauthorized component from causing a consequence of concern.

C-30 VDA COMPONENT INVENTORY
(Informed by NIST SP 800-53 Rev. 4, CM-8, CM-8 (1), CM-8 (2), CM-8 (3), and CM-8 (4))

[Licensee/Applicant]:

- Develops and documents an inventory of VDA components that:
  - Accurately reflects the current VDA;
  - Includes all components within the boundary of the VDA;
  - Is at the level of granularity necessary for tracking and reporting;
  - Includes information necessary to achieve effective VDA component accountability; and
- Reviews and updates the VDA component inventory at least every 92 days or as part of any changes to a VDA;
- Updates the inventory of VDA components as an integral part of component installations, removals, and VDA updates;
- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA;
- Employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components;
- Includes in the VDA component inventory information, a means for identifying individuals responsible/accountable for administering those components; and
- Takes appropriate actions when unauthorized components are detected to remove, disable, or otherwise prevent the unauthorized component from causing a consequence of concern.

C-31 INSTALLED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-11, CM-11 (1), and CM-11 (2))

[Licensee/Applicant]:

- Establishes policies governing the installation of software on VDAs consistent with configuration management in 10 CFR 73.53(f);
- Enforces software installation policies using automated measures where supported;
- Monitors policy compliance using automated measures where supported;
- Ensures appropriate personnel are alerted in near real-time when the unauthorized installation of software is detected on the VDA; and
- Prohibits user installation of software on the VDA without explicit privileged status.

C-32 IDENTIFICATION AND AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-2, IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (8), IA-2 (9), IA-2 (11), IA-2 (12), IA-3, IA-3 (4), and IA-8)

[Licensee/Applicant] ensures the VDA:

- Uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and non-organizational users (or processes acting on behalf of non-organizational users);
- Implements multifactor authentication for network access to privileged accounts;
- Implements multifactor authentication for network access to non-privileged accounts;
- Implements multifactor authentication for local access to privileged accounts;
- Implements multifactor authentication for local access to non-privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to non-privileged accounts;

- Implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets E-authentication Assurance Level 4 as described in NIST SP 800-63-2 or later revisions;
- Accepts and electronically verifies Personal Identity Verification credentials;
- Uniquely identifies and authenticates devices before establishing a connection to a VDA; and
- Ensures that device identification and authentication based on attestation is handled by the configuration management process.

C-33 IDENTIFIER MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-4, IA-4 (2), and IA-4 (7))

[Licensee/Applicant] manages VDA identifiers by:

- Receiving independent management authorization to assign an individual, group, role, or device identifier;
- Selecting an identifier that identifies an individual, group, role, or device;
- Assigning the identifier to the intended individual, group, role, or device;
- Preventing reuse of identifiers where reuse could allow unintended or unauthorized access; and
- Disabling the identifier within 30 days of inactivity.

[Licensee/Applicant] requires that the registration process to receive an individual identifier:

- Includes supervisor authorization; and
- Is conducted in-person before a designated registration authority.

C-34 AUTHENTICATOR MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the organization;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators prior to VDA installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Documenting authenticator types approved for use, the frequency for changing/refreshing, and the technical justification that demonstrates that adequate security is provided by the frequency;
- Protecting authenticator content from unauthorized disclosure and modification;
- Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- Changing authenticators for group/role accounts when membership to those accounts changes.

[Licensee/Applicant] requires that the registration process to receive authenticators be conducted in person or by a trusted third party with management authorization.

C-35 PASSWORD-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (1))

For password-based authentication for the VDA, the [licensee/applicant]:

- Enforces a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security;
- Enforces password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters;
- Enforces a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries;
- Stores and transmits only cryptographically-protected passwords;
- Enforces lifetime restrictions for password minimums of 1 day and provides a technical basis for maximums defined and documented by the CST that prevents unauthorized access;
- Prohibits password reuse for 10 generations;
- Requires an immediate change to a permanent password upon the first logon, when temporary passwords are used for VDA logons;
- Stores written or electronic copies of master passwords in a secure location with limited access; and
- Employs automated tools to determine if password authenticators are sufficiently strong to prevent an adversary from executing a password-guessing attack.

C-36 PUBLIC KEY INFRASTRUCTURE (PKI)-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (2))

[Licensee/Applicant] ensures that PKI-based authentication for the VDA:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group; and
- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

C-37 IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (3))

[Licensee/Applicant] requires that the registration process to receive authenticators be conducted in person or by a trusted third party with management authorization.

C-38 HARDWARE TOKEN-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (11))

[Licensee/Applicant] ensures that hardware token-based authentication for the VDA, employs mechanisms that satisfy Level 4 as described in NIST SP 800-63-2 or later revisions.

C-39 AUTHENTICATOR FEEDBACK
(Informed by NIST SP 800-53 Rev. 4, IA-6)

[Licensee/Applicant] ensures the VDA obscures feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

C-40 CRYPTOGRAPHIC MODULE AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-7)

[Licensee/Applicant] ensures the VDA implements mechanisms for authentication to a cryptographic module based on NIST Cryptographic Module Validation Program (CMVP) and associated guidance for such authentication.

C-41 INCIDENT RESPONSE TRAINING
(Informed by NIST SP 800-53 Rev. 4, IR-2, IR-2 (1), and IR-2 (2))

[Licensee/Applicant] provides incident response training to VDA users consistent with assigned roles and responsibilities:

- Within 92 days of assuming an incident response role or responsibility;
- When required by VDA changes; and
- At least every 12 months.

[Licensee/Applicant]:

- Incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations; and
- Employs automated mechanisms to provide a more thorough and realistic incident response training environment.

C-42 INCIDENT RESPONSE TESTING
(Informed by NIST SP 800-53 Rev. 4, IR-3 and IR-3 (2))

[Licensee/Applicant]:

- Tests the incident response capability for the VDA at least every 92 days using one or more of the following methods to determine the incident response effectiveness and documents the results of checklists, walk-through or tabletop exercises, and simulations (parallel/full interrupt);
- Tests the incident response capability for the VDA at least every 36 months using a comprehensive exercise; and
- Coordinates incident response testing with organizational elements responsible for related plans.

C-43 INCIDENT HANDLING
(Informed by NIST SP 800-53 Rev. 4, IR-4, IR-4 (1), and IR-4 (4))

[Licensee/Applicant]:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities;
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly;
- Employs automated mechanisms to support the incident handling process; and

- Correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

C-44 INCIDENT MONITORING
(Informed by NIST SP 800-53 Rev. 4, IR-5 and IR-5 (1))

[Licensee/Applicant]
- Tracks and documents VDA security incidents; and
- Employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

C-45 INCIDENT REPORTING
(Informed by NIST SP 800-53 Rev. 4, IR-6 and IR-6 (1))

[Licensee/Applicant]:
- Requires personnel to report suspected cyber security incidents to the CST upon discovery; and
- Employs automated mechanisms to assist in the reporting of security incidents.

C-46 INCIDENT RESPONSE ASSISTANCE
(Informed by NIST SP 800-53 Rev. 4, IR-7 and IR-7 (1))

[Licensee/Applicant]:
- Provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the VDA for the handling and reporting of security incidents; and
- Employs automated mechanisms to increase the availability of incident response-related information and support.

C-47 INFORMATION SPILLAGE RESPONSE
(Informed by NIST SP 800-53 Rev. 4, IR-9, IR-9 (1), IR-9 (2), IR-9 (3), and IR-9 (4))

[Licensee/Applicant]:
- Responds to information spills by:
  - Identifying the specific information involved in the information system contamination;
  - Alerting the CST of the information spill using a method of communication not associated with the spill;
  - Isolating the contaminated information system or VDA component;
  - Eradicating the information from the contaminated information system or VDA component;
  - Identifying other VDAs that may have been subsequently contaminated;
  - Documenting the incident; and
- Assigns cleared personnel with responsibility for responding to information spills;
- Provides information spillage response training at least every 12 months;
- Implements procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions; and
- Employs appropriate response procedures and safeguards for personnel exposed to information not within assigned access authorizations.

C-48 CONTROLLED MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-2 and MA-2 (2))

[Licensee/Applicant]:

- Performs and documents maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern;
- Reviews records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days;
- Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Requires that CST approve the removal of the VDA for off-site maintenance or repairs outside the licensees positive control;
- Sanitizes equipment to remove all information from associated media prior to removal for off-site maintenance or repairs outside the licensees positive control;
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions;
- Includes in records of maintenance and repairs on VDA components at a minimum: date, time, identification of those performing the maintenance, description of maintenance performed, and VDA components removed or replaced;
- Retains records for inspection by the NRC;
- Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
- Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

C-49 MAINTENANCE TOOLS
(Informed by NIST SP 800-53 Rev. 4, MA-3, MA-3 (1), MA-3 (2), and MA-3 (3))

[Licensee/Applicant]:

- Approves, controls, and monitors VDA maintenance tools;
- Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications; and
- Checks media containing diagnostic and test programs for malicious code before the media are used in the VDA.

[Licensee/Applicant] prevents the unauthorized removal of maintenance equipment containing VDA information by:

- Verifying that there is no VDA information contained on the equipment;
- Sanitizing or destroying the equipment;
- Retaining the equipment within the facility; or
- Obtaining an exemption from the CST explicitly authorizing removal of the equipment from the facility.

C-50 NONLOCAL MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant]:

- Approves and monitors nonlocal maintenance and diagnostic activities;

- Documents and only allows the use of nonlocal maintenance and diagnostic tools for the VDA where those tools do not introduce vulnerabilities or lead to a consequence of concern (e.g., information systems that perform maintenance on VDAS are protected equivalent to the VDA);
- Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
- Maintains records for nonlocal maintenance and diagnostic activities; and
- Terminates session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant]:

- Documents the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections; or
- Removes the component to be serviced from the VDA prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to VDA information) before removal from licensee facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the VDA.

C-51 MAINTENANCE PERSONNEL
(Informed by NIST SP 800-53 Rev. 4, MA-5, MA-5 (1), and MA-5 (2))

[Licensee/Applicant]:

- Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- Ensures that unescorted personnel performing maintenance on the VDA have required access authorizations;
- Ensures that personnel performing maintenance and diagnostic activities on an VDA processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the VDA;
- Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations;
- Implements procedures for the use of maintenance personnel that lack appropriate security clearances that include the following requirements:
  - Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the VDA by approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
  - Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the VDA are sanitized and all nonvolatile storage media are removed or physically disconnected from the VDA and secured; and
- Develops and implements alternate security safeguards in the event an information VDA component cannot be sanitized, removed, or disconnected from the VDA.

C-52 TIMELY MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-6)

[Licensee/Applicant] obtains maintenance support and/or spare parts for VDAs that must remain operational to prevent a consequence of concern.

C-53 MEDIA ACCESS
(Informed by NIST SP 800-53 Rev. 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media includes any active storage device, passive storage device or passive media that:

- Contain information used to manage, configure, maintain, secure or operate the VDA; or
- Are used on the VDA for any purpose.

C-54 MEDIA MARKING
(Informed by NIST SP 800-53 Rev. 4, MP-3)

[Licensee/Applicant] marks VDA media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

C-55 MEDIA STORAGE
(Informed by NIST SP 800-53 Rev. 4, MP-4)

[Licensee/Applicant]:

- Physically controls and securely stores VDA media; and
- Protects VDA media until the media are destroyed or sanitized using approved equipment, techniques, and procedures that would prevent recovery of the data by an adversary.

C-56 MEDIA TRANSPORT
(Informed by NIST SP 800-53 Rev. 4, MP-5 and MP-5 (4))

[Licensee/Applicant]:

- Protects and controls VDA media during transport outside of controlled areas;
- Maintains accountability for VDA media during transport outside of controlled areas;
- Documents activities associated with the transport of VDA media;
- Restricts the activities associated with the transport of VDA media to authorized personnel; and
- Implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

C-57 MEDIA SANITIZATION
(Informed by NIST SP 800-53 Rev. 4, MP-6, MP-6 (1), MP-6 (2), and MP-6 (3))

[Licensee/Applicant]:

- Sanitizes VDA media prior to disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary;
- Reviews, approves, tracks, documents, and verifies media sanitization and disposal actions;
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information;
- Tests sanitization equipment and procedures at least every 12 months to verify that the intended sanitization is being achieved;
- Applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the VDA; and
- Enforces dual authorization for the sanitization of media.

C-58 MEDIA USE
(Informed by NIST SP 800-53 Rev. 4, MP-7, and MP-7 (1))

[Licensee/Applicant]:

- Prohibits the use of any media with a VDA, except specifically approved VDA media with an identifiable and verifiable owner; and
- Prohibits the use of sanitization-resistant media in any VDA.

C-59 ENHANCEMENTS TO ACCESS CONTROL FOR TRANSMISSION MEDIUM
(Informed by NIST SP 800-53 Rev. 4, PE-4)

[Licensee/Applicant]:

- Monitors physical access to VDA transmission and distribution lines; and
- Reviews VDA transmission and distribution lines physical protection measures for tampering or indications of attempted unauthorized access.

C-60 MONITORING PHYSICAL ACCESS
(Informed by NIST SP 800-53 Rev. 4, PE-6)

[Licensee/Applicant]:

- Monitors physical access to the facility where the VDA resides to detect and respond to physical security incidents;
- Reviews physical access logs in a timely manner and upon occurrence of anomalous behavior;
- Coordinates results of reviews and investigations with the organizational incident response capability; and
- Monitors physical access to the VDA to detect unauthorized access in a timely manner.

C-61 ENHANCEMENT TO CYBER SECURITY ARCHITECTURE
(Informed by NIST SP 800-53 Rev. 4, PL-8 (2))

[Licensee/Applicant] requires that security safeguards are obtained from different suppliers.

C-62 VULNERABILITY SCANNING
(Informed by NIST SP 800-53 Rev. 4, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), RA-5 (5), and RA-5 (8))

[Licensee/Applicant]:

- Scans for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA, applications or both are identified and reported;
- Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures;
  - Measuring vulnerability impact; and
- Analyzes vulnerability scan reports and results from security control assessments;
- Addresses vulnerabilities in a timely and technically justified manner to prevent a consequence of concern;
- Shares information obtained from the vulnerability scanning process and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other VDAs (i.e., systemic weaknesses or deficiencies);

- Employs vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned;
- Updates the VDA vulnerabilities scanned prior to a new scan;
- Employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information VDA components scanned and vulnerabilities checked);
- Determines what information about the VDA is discoverable by adversaries and takes measures to address the associated potential cyber security issues;
- Implements privileged access authorization to the VDA for vulnerability scanning activities; and
- Reviews historic audit logs to determine if a vulnerability identified in the VDA has been previously exploited.

C-63 EXTERNAL INFORMATION SYSTEM SERVICES
(Informed by NIST SP 800-53 Rev. 4, SA-9, SA-9 (2), and SA-9 (3))

[Licensee/Applicant]:

- Requires that providers of external information system services that interact with VDAs comply with information security requirements and address security controls for the associated consequence of concern;
- Defines and documents oversight and user roles and responsibilities with regard to external information system services;
- Employs automated mechanisms to monitor security control compliance by external service providers on an ongoing basis;
- Requires providers of external information system services that interact with VDAs to identify the functions, ports, protocols, and other services required for the use of such services; and
- Establishes, documents, and maintains trust relationships with external service providers through contracts or service-level agreements to provide assurance that external information system services that interact with VDAs the security requirements necessary to address the security controls in this Appendix.

C-64 DEVELOPER CONFIGURATION MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SA-10)

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service to:

- Perform configuration management during the VDA, component, or service lifecycle;
- Document, manage, and control the integrity of changes to the VDA, component, or service;
- Implement only organization-approved changes to the VDA, component, or service;
- Document approved changes to the VDA, component, or service and the potential security impacts of such changes; and
- Track security flaws and flaw resolution within the VDA, component, or service and report findings to CST.

C-65 THIRD-PARTY HARDWARE, SOFTWARE AND FIRMWARE
(Informed by NIST SP 800-53 Rev. 4, SA-10 (1), SA-10 (2), SA-10 (3), SA-10 (6), SA-11 (1), SA-11 (2), SA-11 (3), SA-11 (4), SA-11 (5), SA-11 (6), SA-11 (7), and SA-11 (8))

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service to:

- Create and implement a security assessment plan to include, at a minimum:
  - Integrity verification of hardware, software and firmware components;
  - Ensuring that security-relevant hardware, software, and firmware updates distributed to the [Licensee/Applicant] are exactly as specified by the master copies;

  - Static and dynamic code analysis using tools and techniques that identify common flaws (including manual code review) and document the results of the analysis;
  - Threat and vulnerability analyses and subsequent testing/evaluation of the as-built VDA, component, or service;
  - Full penetration testing;
  - Attack surface review;
  - Verify that the scope of security testing/evaluation provides complete coverage of required security controls; and
- Perform comprehensive cyber security testing and evaluation;
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing/evaluation.

C-66 DEVELOPER SECURITY TESTING AND EVALUATION
(Informed by NIST SP 800-53 Rev. 4, SA-11)

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service to:
- Create and implement a security assessment plan;
- Perform comprehensive cyber security testing and evaluation;
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing/evaluation.

C-67 ENHANCEMENTS TO SUPPLY CHAIN PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SA-12 (1), SA-12 (2), SA-12 (9), SA-12 (10), and SA-12 (14))

[Licensee/Applicant]:
- Utilizes acquisition strategies, contract tools, and procurement methods for the purchase of the VDA, VDA component, or VDA service from suppliers to reinforce supply chain protection;
- Conducts a supplier review prior to entering into a contractual agreement to acquire the VDA, VDA component, or VDA service;
- Utilizes operations security safeguards in accordance with classification guides to protect supply chain-related information for the VDA, VDA component, or VDA service;
- Utilizes security safeguards to validate that the VDA received is genuine and has not been altered; and
- Establishes and retains unique identification of supply chain elements, processes, and actors for the VDA, VDA component, or VDA service.

C-68 TRUSTWORTHINESS
(Informed by NIST SP 800-53 Rev. 4, SA-13)

When acquiring, designing, developing, or implementing VDAs, the [licensee/applicant]:
- Describes the level of required trustworthiness required in the VDA to meet security requirements; and
- Implements measures to achieve, measure and document such trustworthiness.

C-69 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
(Informed by NIST SP 800-53 Rev. 4, SA-15)

[Licensee/Applicant]:

- Requires the developer of the VDA, VDA component, or VDA service to follow a documented development process that:
  - Explicitly addresses security requirements;
  - Identifies the standards and tools used in the development process;
  - Documents the specific tool options and tool configurations used in the development process; and
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy VDA security requirements.

C-70 THIRD-PARTY DEVELOPER PROCESS, STANDARDS, AND TOOLS
(Informed by NIST SP 800-53 Rev. 4, SA-15 (1), SA-15 (2), SA-15 (3), SA-15 (4), SA-15 (5), SA-15 (6), and SA-15 (7))

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service to:

- Define quality metrics at the beginning of the development process;
- Provide evidence of meeting the quality metrics upon delivery;
- Select and employ a security tracking tool for use during the development process;
- Perform a criticality analysis;
- Perform threat modeling and a vulnerability analysis ;
- Reduce attack surfaces;
- Implement an explicit process to continuously improve the development process; and
- Perform an automated vulnerability analysis;
  - Determine the exploitation potential for discovered vulnerabilities;
  - Determine potential risk mitigations for delivered vulnerabilities; and
  - Deliver the outputs of the tools and results of the analysis to the CST.

C-71 DEVELOPER SECURITY ARCHITECTURE AND DESIGN
(Informed by NIST SP 800-53 Rev. 4, SA-17)

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service e to produce a design specification and security architecture that:

- Is consistent with and supportive of the licensee's security architecture;
- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

C-72 THIRD-PARTY DEVELOPER SECURITY ARCHITECTURE AND DESIGN
(Informed by NIST SP 800-53 Rev. 4, SA-17 (1) and SA-17 (2))

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service to:

- Produce, as an integral part of the development process, a formal policy model describing how security controls in this Appendix are met;

- Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented;
- Define security-relevant hardware, software, and firmware; and
- Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

C-73 TAMPER RESISTANCE AND DETECTION
(Informed by NIST SP 800-53 Rev. 4, SA-18, SA-18 (1), and SA-18 (2))

[Licensee/Applicant]:
- Implements a tamper protection program for the VDA, VDA component, or VDA service;
- Employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance; and
- Inspects VDA and VDA components randomly, but at least every hour, to detect tampering.

C-74 COMPONENT AUTHENTICITY
(Informed by NIST SP 800-53 Rev. 4, SA-19)

[Licensee/Applicant]:
- Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the VDA;
- Reports counterfeit information VDA components to the NRC and relevant law enforcement agencies;
- Trains CST personnel to detect counterfeit information VDA components (including hardware, software, and firmware); and
- Scans for counterfeit information VDA components during VDA validation activities.

C-75 DEVELOPER SCREENING
(Informed by NIST SP 800-53 Rev. 4, SA-21 and SA-21 (1))

[Licensee/Applicant] requires that the developer of the VDA, VDA component or VDA service:
- Have appropriate access authorizations;
- Satisfy licensee personnel security requirements; and
- Document and provide for inspection and assessment to ensure that the required access authorizations and screening criteria are satisfied.

C-76 UNSUPPORTED VDA COMPONENTS
(Informed by NIST SP 800-53 Rev. 4, SA-22 and SA-22 (1))

[Licensee/Applicant]:
- Replaces information VDA components when support for the components is no longer available from the developer, vendor, or manufacturer;
- Provides justification and documents approval for the continued use of unsupported VDA components required to satisfy mission/business needs; and
- Retains support for unsupported information VDA components either in-house or through an approved and validated external third-party.

C-77 SYSTEM PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-2, SC-2 (1), SC-3, SC-3 (1), SC-3 (2), and SC-4)

[Licensee/Applicant]:

- Separates user functionality on the VDA (including user interface services) from VDA management functionality;
- Isolates security functions from nonsecurity functions on the VDA;
- Prevents unauthorized and unintended information transfer via shared resources;
- Prevents the presentation of VDA management-related functionality at an interface for non-privileged users;
- Utilizes underlying hardware separation mechanisms to implement security function isolation; and
- Isolates security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

C-78 DENIAL OF SERVICE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-5)

[Licensee/Applicant] protects against or limits the effects of denial of service attacks by employing technical safeguards and countermeasures.

C-79 BOUNDARY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-7 and SC-7 (3), SC-7 (4), SC-7 (5), SC-7 (7). SC-7 (8), SC-7 (10), SC-7 (11), SC-7 (12), SC-7 (14), SC-7 (18), SC-7 (20), and SC-7 (21))

[Licensee/Applicant] ensures the VDA:

- Denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception);
- Fails securely and safely in the event of an operational failure of a boundary protection device; and
- Monitors and controls communications at the boundary of the VDA and at key internal boundaries within the VDA.

[Licensee/Applicant]:

- Provides the capability to dynamically isolate/segregate VDAs from other VDAs;
- prohibits external network connections to the VDA;
- Protects against unauthorized physical connections to the VDA;
- Allows only incoming communications from authorized sources to be routed to VDAs;
- Implements host-based firewalls on VDAs;
- Protects against unauthorized physical connections to the VDA; and
- Employs boundary mechanisms.

[Licensee/Applicant], for boundary control devices:

- Establishes a traffic flow policy for each interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

- Reviews exceptions to the traffic flow policy at least every 30 days and removes exceptions that are no longer supported by an explicit mission/business need;
- Allows only incoming communications from authorized sources to be routed to VDAs;
- Implements host-based firewalls on VDAs;
- Provides the capability to dynamically isolate/segregate VDAs from other VDAs; and
- Ensures the VDA denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

C-80 EXTERNAL TELECOMMUNICATIONS SERVICES
(Informed by NIST SP 800-53 Rev. 4, SC-7 (4), SC-7 (5), SC-7 (7), SC-7 (8), SC-7 (10), SC-7 (11), SC-7 (12), SC-7 (14), SC-7 (18), SC-7 (20), and SC-7 (21))

[Licensee/Applicant]:

- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- Reviews exceptions to the traffic flow policy on a timely basis and removes exceptions that are no longer supported by an explicit mission/business need;
- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- Reviews exceptions to the traffic flow policy at least every 30 days and removes exceptions that are no longer supported by an explicit mission/business need;
- Prevents the unauthorized exfiltration of information across managed interfaces;
- Allows only incoming communications from authorized sources to be routed to VDAs;
- Implements host-based firewalls on VDAs;
- Protects against unauthorized physical connections to the VDA; and
- Employs boundary protection mechanisms.

[Licensee/Applicant] ensures the VDA:

- Has managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception);
  - Prevents, in conjunction with a remote device, the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks;
- Routes internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
- Provides the capability to dynamically isolate/segregate VDAs from other VDAs;
- Fails securely and safely in the event of an operational failure of a boundary protection device.

C-81 TRANSMISSION CONFIDENTIALITY AND INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures the VDA:

- Protects the confidentiality and integrity of transmitted information; and
- Implements cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to information during transmission, unless the transmission medium is otherwise protected by alternative physical safeguards.

C-82 NETWORK DISCONNECT
(Informed by NIST SP 800-53 Rev. 4, SC-10)

[Licensee/Applicant] terminates the network connection associated with a VDA communications session at the end of the session or within 10 minutes of inactivity, except for communications sessions that are necessary for safe operation of the VDA or are necessary to prevent a consequence of concern.

C-83 TRUSTED PATH
(Informed by NIST SP 800-53 Rev. 4, SC-11 and SC-11 (1))

[Licensee/Applicant] establishes a trusted VDA communications path between the user and the security functions of the VDA to include, at a minimum, authentication and re-authentication.

[Licensee/Applicant] provides a trusted VDA communications path that is logically isolated and distinguishable from other paths.

C-84 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SC-12 and SC-12 (1))

[Licensee/Applicant]:

- Establishes and manages cryptographic keys for required cryptography employed within the VDA in accordance with NIST CMVP; and
- Maintains availability of information necessary to safely operate the VDA or prevent a consequence of concern in the event of the loss of cryptographic keys by users.

C-85 COLLABORATIVE COMPUTING DEVICES
(Informed by NIST SP 800-53 Rev. 4, SC-15, SC-15 (1), SC-15 (3), and SC-15 (4))

[Licensee/Applicant] disables or removes collaborative computing devices from digital assets in areas where access could disclose information leading to a consequence of concern.

[Licensee/Applicant] ensure the VDA:

- Prohibits remote activation of collaborative computing devices except where explicitly authorized;
- Provides an explicit indication of use to users physically present at the devices;
- Provides physical disconnect of collaborative computing devices in a manner that supports ease of use; and
- Provides an explicit indication of current participants in collaborative sessions.

C-86 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
(Informed by NIST SP 800-53 Rev. 4, SC-17)

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

C-87 VOICE OVER INTERNET PROTOCOL (VOIP)
(Informed by NIST SP 800-53 Rev. 4, SC-19)

[Licensee/Applicant]:

- Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the VDA if used maliciously; and
- Authorizes, monitors, and controls the use of VoIP within the VDA.

C-88 SECURE NAME / ADDRESS RESOLUTION
(Informed by NIST SP 800-53 Rev. 4, SC-20, SC-20a, SC-20 (2), SC-21, and SC-22)

[Licensee/Applicant] ensures the VDA:

- Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the VDA returns in response to external name/address resolution queries;
- Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace;
- Requests and performs data origin authentication and data integrity verification on the name/address resolution responses the VDA receives from authoritative sources;
- Collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation; and
- Provides data origin and integrity protection artifacts for internal name/address resolution queries.

C-89 SESSION AUTHENTICITY
(Informed by NIST SP 800-53 Rev. 4, SC-23)

[Licensee/Applicant] ensures the VDA protects the authenticity of communications sessions.

C-90 FAIL IN KNOWN STATE
(Informed by NIST SP 800-53 Rev. 4, SC-24)

[Licensee/Applicant]:

- Ensures VDAs fail in a known-state to ensure that functions are not adversely impacted; and
- Prevents a loss of confidentiality, integrity, or availability in the event of a failure of the VDA or a component of the VDA.

C-91 HONEYPOTS
(Informed by NIST SP 800-53 Rev. 4, SC-26)

[Licensee/Applicant] ensures the VDA includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

C-92 PROTECTION OF INFORMATION AT REST
(Informed by NIST SP 800-53 Rev. 4, SC-28)

[Licensee/Applicant] ensures the VDA:

- Protects the confidentiality and integrity of VDA information at rest; and
- Implements cryptographic mechanisms to prevent unauthorized disclosure and modification of VDA information.

C-93 OPERATIONS SECURITY
(Informed by NIST SP 800-53 Rev. 4, SC-38)

[Licensee/Applicant] employs operations security safeguards to protect VDA information throughout the system development life cycle.

C-94 PROCESS ISOLATION
(Informed by NIST SP 800-53 Rev. 4, SC-39)

[Licensee/Applicant] maintains a separate execution domain for each executing process.

C-95 PORT AND I/O DEVICE ACCESS
(Informed by NIST SP 800-53 Rev. 4, SC-41)

[Licensee/Applicant] physically disables or removes unused ports or input/output devices on VDAs and VDA components.

C-96 FLAW REMEDIATION
(Informed by NIST SP 800-53 Rev. 4, SI-2, SI-2 (1), and SI-2 (2))

[Licensee/Applicant]:

- Identifies, reports, and corrects VDA flaws;
- Implement interim compensatory measure following identification of the flaw;
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- Correcting the flaw expeditiously using the configuration management process;
- Incorporates flaw remediation into the organizational configuration management process;
- Performs vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production;
- Centrally manages the flaw remediation process; and
- Employs automated mechanisms to determine the state of VDA components with regard to flaw remediation.

C-97 MALICIOUS CODE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-3, SI-3 (1), SI-3 (2), SI-3 (8), and SI-2 (10))

[Licensee/Applicant]:

- Employs malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code;
- Updates malicious code protection mechanisms whenever new releases are available;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the VDA at least every 7 days;

  - Perform real-time scans of files from external sources as the files are downloaded, opened, or executed;
  - Prevent malicious code execution;
  - Alert the CST of the detection of malicious code in a timely manner; and
- Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA;
- Centrally manages malicious code protection mechanisms;
- Automatically updates malicious code protection mechanisms for the VDA;
- Detects unauthorized operating system commands in VDAs through the kernel application programming interface and:
  - Issues a warning;
  - Audits the command execution;
  - Prevents the execution of the command; and
- Employs tools and techniques to analyze the characteristics and behavior of malicious code; and
- Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

C-98 VDA MONITORING

(Informed by NIST SP 800-53 Rev. 4, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-4 (9), SI-4 (10), SI-4 (11), SI-4 (12), SI-4 (13), SI-4 (14), SI-4 (15), SI-4 (16), SI-4 (17), SI-4 (19), SI-4 (20), SI-4 (21), SI-4 (22), SI-4 (23), and SI-4 (24))

[Licensee/Applicant]:

- Monitors the VDA to detect:
  - Cyber attacks and indicators of potential cyber attacks;
  - Unauthorized local, network, and remote connections; and
- Identifies unauthorized use of the VDA using automated or other means;
- Utilizes internal and external monitoring of VDAs to ensure adequate capability to detect cyber attacks and indicators of compromise;
- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- Heightens the level of VDA monitoring activity whenever there is an indication of increased risk to the facility or VDAs that can result in a consequence of concern, based on law enforcement information, intelligence information, or other credible sources of information;
- Provides VDA monitoring information to appropriate licensee cyber security personnel as necessary;
- Employs automated tools to support near real-time analysis of events;
- Monitors inbound and outbound VDA communications traffic in near real-time for unusual or unauthorized activities or conditions;
- Ensures appropriate cyber security personnel are alerted when indications of compromise or potential compromise of a VDA occurs;
- Tests intrusion-monitoring tools at least every 92 days;
- Makes provisions so that encrypted communications traffic is visible to authorized network monitoring tools;
- Analyzes outbound communications traffic for VDAs at the external boundary and selected interior points within the boundary to discover anomalies;
- Employs automated mechanisms to alert security personnel, in a timely manner, of inappropriate or unusual activities with security implications;
- Analyzes communications traffic/event patterns for the VDA;

- Develops profiles representing common traffic patterns and/or events;
- Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives;
- Employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the VDA;
- Employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks;
- Correlates information from monitoring tools employed throughout the VDA;
- Correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness;
- Implements additional monitoring of: privileged users, probationary personnel, and individuals determined to be high-risk;
- Detects VDA network services that have not been authorized or approved and alerts appropriate personnel in a timely manner;
- Implements host-based monitoring mechanisms; and
- Discovers, collects, distributes, and uses indicators of VDA compromise.

C-99 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
(Informed by NIST SP 800-53 Rev. 4, SI-5 and SI-5 (1))

[Licensee/Applicant]:

- Receives cyber security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis;
- Generates internal security alerts, advisories, and directives as necessary to prevent a consequence of concern;
- Disseminates security alerts, advisories, and directives to appropriate personnel and the NRC;
- Implements security directives in a timely manner; and
- Employs automated mechanisms to make security alert and advisory information available throughout the organization.

C-100 SECURITY FUNCTION VERIFICATION
(Informed by NIST SP 800-53 Rev. 4, SI-6 and SI-6 (3))

[Licensee/Applicant] ensures the VDA:

- Verifies the correct operation of security functions;
- Performs this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and when anomalies are discovered; and
- Notifies appropriate personnel in a timely manner of failed security verification tests.

[Licensee/Applicant] reports the results of security function verification to the CST.

C-101 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SI-7, SI-7 (1), SI-7 (2), SI-7 (5), SI-7 (7), SI-7 (12), SI-7 (12), SI-7 (14))

[Licensee/Applicant]:

- Employs integrity verification tools to detect unauthorized changes to VDA software, firmware, and information;

- Performs an integrity check of VDA software, firmware, and information. This occurs, where possible, upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and when anomalies are discovered;
- Employs automated tools that provide notification to appropriate personnel upon discovering discrepancies during integrity verification;
- Automatically takes proactive protection measures when VDA integrity violations are discovered;
- Incorporates the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability;
- Requires that the integrity of software be verified prior to execution; and
- Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.

C-102 ENHANCEMENTS TO INFORMATION INPUT VALIDATION
(Informed by NIST SP 800-53 Rev. 4, SI-10 (3) and SI-10 (5))

[Licensee/Applicant]:

- Ensures the VDA behaves in a predictable and documented manner when invalid inputs are received; and
- Restricts the use of information inputs to defined trusted sources and defined formats.

C-103 ERROR HANDLING
(Informed by NIST SP 800-53 Rev. 4, SI-11)

[Licensee/Applicant] ensures the VDA:

- Generates VDA error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- Reveals VDA error messages only to authorized personnel with a need-to-know.

C-104 INFORMATION HANDLING AND RETENTION
(Informed by NIST SP 800-53 Rev. 4, SI-12)

[Licensee/Applicant] handles and retains information within the VDA and information output from the VDA, in accordance with NRC record retention requirements.

C-105 MEMORY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-16)

[Licensee/Applicant] implements automated mechanisms and safeguards for the VDA to protect its memory from unauthorized code execution.

APPENDIX D

ADDITIONAL CYBER SECURITY CONTROLS FOR VITAL DIGITAL ASSETS ASSOCIATED WITH LATENT CONSEQUENCES OF CONCERN – SAFEGUARDS (CATEGORY II FACILITIES ONLY)

D-1 INSIDER THREAT PROGRAM

(Informed by National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, PM-12 and AT-2 (2))

[Licensee/Applicant] implements an insider threat program that includes a cross-discipline insider threat incident handling team. [Licensee/Applicant] includes security awareness training on recognizing and reporting potential indicators of insider threat.

D-2 ACCOUNT MANAGEMENT PROCEDURES

(Informed by NIST SP 800-53 Rev. 4, AC-2)

[Licensee/Applicant] employs, at a minimum, the following measures in support of the management of user accounts on vital digital assets (VDAs):

- Assigns account managers for VDA accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires independent management approval for requests to create VDA accounts;
- Creates, enables, modifies, disables, and removes VDA accounts in accordance with the Access Control policy;
- Monitors the use of VDA accounts;
- Notifies account managers in a timely manner:
  - When accounts are no longer required;
  - When users are terminated or transferred;
  - When individual VDA usage or need-to-know changes; and
- Authorizes access to the VDA based on:
  - A valid access authorization;
  - Intended VDA usage; and
- Reviews accounts at least every 30 days for compliance with account management requirements; and
- Employs, at a minimum, the following measures to restrict the creation and issuance of shared/group VDA accounts:
  - Ensures shared/group account requests:
    - Are issued only when necessary to prevent a consequence of concern;
    - Include a documented technical justification;
    - Are reviewed and approved by the Cyber Security Team (CST) prior to issuance; and
  - Automatically terminates and establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

D-3 ACCOUNT MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-2 (5), AC-2 (12), and AC-2 (13))

[Licensee/Applicant] employs, at minimum, the following measures in support of the management of VDA accounts using a combination of procedural activity and automated means:

- Requires that users log out within 15 minutes of inactivity unless the login session must be maintained to prevent a consequence of concern;
- Monitors VDA accounts for atypical usage and anomalous activity that could indicate account compromise;
- Reports atypical usage of VDA accounts to the CST; and
- Disables user accounts that have been potentially compromised upon discovery.

D-4 AUTOMATED ACCOUNT MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-2 (1), AC-2 (2), AC-2 (3), and AC-2 (4))

[Licensee/Applicant] employs, at minimum, the following automated technical mechanisms to support the management of VDA accounts including:

- Automatically removes or disables temporary and emergency accounts once they are no longer needed;
- Automatically disables inactive accounts within 30 days; and
- Automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate personnel in a timely manner.

D-5 ACCESS MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-3 and AC-4)

[Licensee/Applicant] ensures the VDA employs technical measures in support of the enforcement of account access to enforce approved authorizations for:

- Logical access to VDA information and VDA resources in accordance with applicable access control policies; and
- Controlling the flow of information within the VDA and between interconnected systems and VDAs.

D-6 SECURITY ATTRIBUTES
(Informed by NIST SP 800-53 Rev. 4, AC-16, AC-16 (1), AC-16 (4), and SC-16)

[Licensee/Applicant]:

- Provides the means to associate security attributes with information in storage, in process, and/or in transmission;
- Ensures that the security attribute associations are made and retained with the information;
- Establishes the permitted security attributes for VDAs;
- Determines the permitted values or ranges for each of the established security attributes;
- Supports the association of VDA security attributes with information exchanged or transmitted between digital assets, VDAs, and components; and
- Validates the integrity of transmitted security attributes for the VDA.

D-7 REMOTE ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-17)

[Licensee/Applicant]:

- Establishes and documents usage restrictions, configurations, connection requirements, and implementation guidance for each type of remote access allowed; and
- Authorizes remote access to the VDA prior to allowing such connections.

D-8 MANAGED ACCESS CONTROL POINTS
(Informed by NIST SP 800-53 Rev. 4, AC-17 (3))

[Licensee/Applicant]

- Prohibits all remote access to VDAs associated with security functions; and
- Ensures all remote accesses to non-security related VDAs is through a boundary control device meeting the requirements in cyber security control, "BOUNDARY PROTECTION," of this Appendix.

D-9 WIRELESS ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-18)

[Licensee/Applicant]:

- Establishes usage restrictions, configurations, connection requirements, and implementation guidance for wireless access; and
- Authorizes wireless access to the VDA prior to allowing such connections.

D-10 RESTRICT CONFIGURATIONS BY USERS
(Informed by NIST SP 800-53 Rev. 4, AC-18 (4))

[Licensee/Applicant] identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

D-11 ANTENNAS AND TRANSMISSION POWER LEVELS
(Informed by NIST SP 800-53 Rev. 4, AC-18 (5))

[Licensee/Applicant] selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be accessed outside of licensee-controlled boundaries.

D-12 EXTERNAL INFORMATION SHARING
(Informed by NIST SP 800-53 Rev. 4, AC-21)

When VDA information is shared with external parties, [licensee/applicant]:

- Ensures that access authorizations assigned to the sharing partner match the access restrictions on the information; and
- Employs automated mechanisms to enforce these restrictions.

D-13 USE OF EXTERNAL INFORMATION SYSTEMS
(Informed by NIST SP 800-53 Rev. 4, AC-20, AC-20 (1), AC-20 (2), and AC-20 (4))

[Licensee/Applicant] establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- Access the VDA from external information systems; and
- Process, store, or transmit organization-controlled information using external information systems.

[Licensee/Applicant]:

- Restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems;
- Prohibits the use of organization-controlled network accessible storage devices] in external information systems; and
- Permits authorized individuals to use an external information system to access the VDA or to process, store, or transmit organization-controlled information only when the [licensee/applicant]:
  - Verifies the implementation of security controls on the external system equivalent to security controls addressed for the VDA; or
  - Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

D-14 AUDIT DATA DEFINITION, GENERATION, AND CONTENT
(Informed by NIST SP 800-53 Rev. 4, AU-3, AU-3 (1), AU-3 (2), AU-5, AU-5 (2), AU-12, AU-12 (3), AU-14, AU-14 (1), and AU-14 (2))

[Licensee/Applicant] ensures the VDA:

- Generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event; and
- Generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum:
  - Account (user or service) login failure;
  - Account role or privilege change;
  - File or object creation, modification and deletion;
  - Service start and stop;
  - Privileged service call;
  - Account creation and modification;
  - Account right assignment;
  - Audit policy change;
  - User account password change;
  - User group creation and modification; and
  - Remote session start and failure.

[Licensee/Applicant] ensures the VDA auditing function:

- Alerts cyber security personnel in near real-time of an audit processing failure, or where audit failure events occur that could indicate VDA compromise;
- Takes automated measures to preserve audit data;
- Provides the capability to increase or modify audit record content in response to threat intelligence;

- Initiates session audits at VDA start-up;
- Provides the capability for authorized users to select a user session to capture/record or view/hear;
- Provides the capability for authorized users to capture/record and log content related to a user session; and
- Provides centralized management and configuration of the content to be captured in audit records.

D-15 AUDIT DATA MANAGEMENT AND PROTECTION
(Informed by NIST SP 800-53 Rev. 4, AU-4, AU-5 (1), AU-9, AU-9 (2), AU-9 (3), AU-9 (4), and AU-10)

[Licensee/Applicant]:

- Allocates sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configures auditing to prevent capacity from being exceeded;
- Authorizes access to management of audit functionality to only authorized users with cyber security responsibilities;
- Ensures the VDA provides an alert to authorized personnel when allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity;
- Ensures the VDA backs up audit records onto a physically different VDA than the VDA being audited;
- Ensures the VDA protects audit information and audit tools from unauthorized access, modification, and deletion;
- Ensures the VDA implements cryptographic mechanisms to protect the integrity of audit information and audit tools; and
- Ensures the VDA protects against an individual (or process acting on behalf of an individual) falsely denying having performed any action on the VDA.

D-16 AUDIT REVIEW, ANALYSIS, AND REPORTING
(Informed by NIST SP 800-53 Rev. 4, AU-6, AU-6a, AU-6b, AU-6 (1), AU-6 (3), AU-6 (5), AU-6 (6), AU-10 (3), AU-10 (4), and AU-12 (1))

[Licensee/Applicant]:

- Employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities;
- Reviews and analyzes VDA audit records in a timely manner for indications of potential compromise;
- Analyzes and correlates audit records across different repositories to gain organization-wide situational awareness;
- Integrates analysis of audit records with analysis of vulnerability scanning information, performance data, VDA monitoring information, and data/information collected from other sources to further enhance the ability to identify potential unauthorized activity;
- Correlates information from audit records with information obtained from monitoring physical access to the VDA to further enhance the ability to identify potential unauthorized activity;
- Reports findings to the CST; and
- Ensures the VDA compiles audit records into a logical or physical audit trail that is time-correlated to, at a minimum, within one-tenth of a second.

[Licensee/Applicant] ensures the VDA:

- Maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released;

- Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer; and
- Prevents access to, modification of, or transfer of the information in the event of a validation error.

D-17 SECURITY CONTROL ASSESSMENTS
(Informed by NIST SP 800-53 Rev. 4, CA-2)

[Licensee/Applicant]:

- Develops a security assessment plan that describes the scope of the assessment including:
  - Security controls and control enhancements under assessment;
  - Assessment procedures to be used to determine security control effectiveness;
  - Assessment environment, assessment team, and assessment roles and responsibilities; and
- Assesses the security controls in the VDA and its environment of operation at least every 92 days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
- Produces a security assessment report that documents the results of the assessment;
- Includes and documents as part of VDA security control assessments:
  - An attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
  - Announced assessments:
    - In-depth monitoring (to be done automatically, in real time);
    - Vulnerability scanning (to be done at least every 30 days);
    - Malicious actor testing (to be done at least every 92 days);
    - Insider threat assessment (to be done at least every 92 days); and
  - Unannounced assessments (in addition to announced assessments above):
    - Vulnerability scanning (to be done at least every 183 days);
    - Malicious actor testing (to be done at least every 12 months);
    - Insider threat assessment (to be done at least every 183 days);
    - Performance/load testing (to be done at least every 183 days); and
  - Provides the results of the security control assessment to the CST; and
- Restricts access to the results of the security control assessment to authorized personnel with a need-to-know.

D-18 INDEPENDENCE OF ASSESSORS
(Informed by NIST SP 800-53 Rev. 4, CA-2 (1), CA-7 (1), CA-8, and CA-8 (1))

[Licensee/Applicant]:

- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to conduct assessments of the cyber security controls;
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to monitor the cyber security controls for the VDA on an ongoing basis;
- Conducts penetration testing at least every 12 months on the VDA; and
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to perform penetration testing on the VDA.

D-19 ENHANCEMENTS TO VDA CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant]:

- Prohibits remote access to VDAs associated with security functions;
- Employs a "deny-all, permit-by-exception" policy for allowing non-security related VDAs to connect to external information systems;
- Prohibits the direct connection of a non-security related VDA to an external network without the use of:
  - At least one separate, intervening access control device (e.g. firewall, cross domain solution);
  - At least one separate, intervening intrusion detection/prevention mechanism with near real-time prevention, detection and alerting capability;
  - Host-based protective measures;
  - Other measures necessary to prevent a consequence of concern; and
- Prohibits the direct connection of a VDA to a public network;
- Authorizes connections to the VDA; and
- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

D-20 INTERIM COMPENSATORY MEASURES
(Informed by NIST SP 800-53 Rev. 4, CA-5)

[Licensee/Applicant]:

- Documents an interim compensatory measure plan to correct weaknesses or deficiencies noted during the assessment of VDA security controls and to reduce or eliminate known vulnerabilities in the VDA;
- Updates interim compensatory measure plan at least every 30 days based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities; and
- Restricts access to the interim compensatory measure plan to authorized personnel with a need-to-know.

D-21 CONFIGURE VDAS FOR HIGH-RISK AREAS
(Informed by NIST SP 800-53 Rev. 4, CM-2 (7))

Prior to transporting VDAs to locations that [licensee/applicant] deems to be of significant risk, the [licensee/applicant]:

- Documents a detailed justification for the VDA to be transported;
- Obtains written approval from the CST and management;
- Documents the VDA configuration baseline and component inventory prior to leaving controlled areas;
- Ensures safeguards or security-related information on the VDA is purged or protected in a manner that prevents an adversary from recovering the data prior to leaving controlled areas;
- Performs a review of the VDA configuration baseline and component inventory upon return;
- Performs testing of the VDA to ensure no cyber compromise has occurred; and
- Performs a security control assessment to ensure all controls are in place, operational, and performing the intended function.

D-22 CONFIGURATION CHANGE CONTROL
(Informed by NIST SP 800-53 Rev. 4, CM-3)

[Licensee/Applicant]:

- Documents changes to the VDA that will be configuration-controlled per Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53;
- Reviews proposed configuration-controlled changes to the VDA and approves or disapproves such changes with explicit consideration for security impact analyses before implementation of the change;
- Documents configuration change decisions associated with the VDA;
- Implements approved configuration-controlled changes to the VDA;
- Retains records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements;
- Audits and reviews activities associated with configuration-controlled changes to the VDA; and
- Coordinates and provides oversight for configuration change control activities through the change management process.

D-23 CHANGE TESTING AND ANALYSIS
(Informed by NIST SP 800-53 Rev. 4, CM-3 (2), CM-4, and CM-4 (1))

[Licensee/Applicant]:

- Tests, validates, and documents changes to the VDA before implementing the changes to the VDA;
- Analyzes changes to the VDA to determine potential security impacts prior to change implementation; and
- Analyzes changes to the VDA in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

D-24 ACCESS RESTRICTIONS FOR CHANGE
(Informed by NIST SP 800-53 Rev. 4, CM-5 and CM-5 (1))

[Licensee/Applicant]:

- Defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the VDA; and
- Ensures VDA enforces access restrictions and supports auditing of the enforcement actions.

D-25 REVIEW VDA CHANGES
(Informed by NIST SP 800-53 Rev. 4, CM-5 (2))

[Licensee/Applicant] reviews VDA changes at least every 183 days or in the event of suspected compromise to determine whether unauthorized changes have occurred.

D-26 SIGNED COMPONENTS
(Informed by NIST SP 800-53 Rev. 4, CM-5 (3))

[Licensee/Applicant] ensures the VDA prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

D-27 CONFIGURATION SETTINGS
(Informed by NIST SP 800-53 Rev. 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant]:

- Establishes and documents configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves any deviations from established configuration settings;
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;
- Employs automated mechanisms to centrally manage, apply, and verify VDA configuration settings; and
- Reports unauthorized changes to VDA configuration settings to the cyber security incident response team upon detection.

D-28 LEAST FUNCTIONALITY
(Informed by NIST SP 800-53 Rev. 4, CM-7)

[Licensee/Applicant]:

- Configures the VDA to provide only essential capabilities, to perform its function and maintain safe and secure operations; and
- Prohibits or restricts the use of unneeded functions, ports, protocols, and/or services.

D-29 PERIODIC REVIEW
(Informed by NIST SP 800-53 Rev. 4, CM-7 (1))

[Licensee/Applicant]:

- Reviews the VDA at least every 30 days to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
- Disables or restricts unneeded functions, ports, protocols, and/or services identified by the review.

D-30 AUTHORIZED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-7 (2) and CM-7 (4))

[Licensee/Applicant]:

- Identifies software programs authorized to execute on the VDA;
- Employs an "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA;
- Reviews and updates the list of authorized software programs, at least every 183 days; and
- Employs automated mechanisms for the VDA (i.e. application white-listing) to prevent unauthorized program execution.

D-31 VDA COMPONENT INVENTORY
(Informed by NIST SP 800-53 Rev. 4, CM-8, CM-8 (1), CM-8 (2), CM-8 (3), and CM-8 (4)

[Licensee/Applicant]:

- Develops and documents an inventory of VDA components that:
  - Accurately reflects the current VDA;
  - Includes all components within the boundary of the VDA;

  - Is at the level of granularity necessary for tracking and reporting;
  - Includes information necessary to achieve effective VDA component accountability; and
- Reviews and updates the VDA component inventory at least every 92 days or as part of any changes to a VDA;
- Updates the inventory of VDA components as an integral part of component installations, removals, and VDA updates;
- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA;
- Employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components;
- Includes in the VDA component inventory information, a means for identifying individuals responsible/accountable for administering those components; and
- Takes appropriate actions when unauthorized components are detected to remove, disable, or otherwise prevent the unauthorized component from causing a consequence of concern.

D-32 INSTALLED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-11)

[Licensee/Applicant]:
- Establishes policies governing the installation of software on VDAs consistent with configuration management in 10 CFR 73.53(f);
- Enforces software installation policies using automated measures where supported; and
- Monitors policy compliance using automated measures where supported.

D-33 IDENTIFICATION AND AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-2, IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (8), IA-2 (9), IA-2 (11), IA-2 (12), IA-3, and IA-8)

[Licensee/Applicant] ensures the VDA:
- Uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and non-organizational users (or processes acting on behalf of non-organizational users);
- Implements multifactor authentication for network access to privileged accounts;
- Implements multifactor authentication for network access to non-privileged accounts;
- Implements multifactor authentication for local access to privileged accounts;
- Implements multifactor authentication for local access to non-privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to non-privileged accounts;
- Implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the VDA gaining access and the device meets E-authentication Assurance Level 3 as described in NIST SP 800-63-2 or later revisions;
- Accepts and electronically verifies Personal Identity Verification credentials; and
- Uniquely identifies and authenticates devices before establishing a connection to a VDA.

D-34 IDENTIFIER MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-4)

[Licensee/Applicant] manages VDA identifiers by:

- Receiving independent management authorization to assign an individual, group, role, or device identifier;
- Selecting an identifier that identifies an individual, group, role, or device;
- Assigning the identifier to the intended individual, group, role, or device;
- Preventing reuse of identifiers where reuse could allow unintended or unauthorized access; and
- Disabling the identifier within 30 days of inactivity.

D-35 AUTHENTICATOR MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the organization;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators prior to VDA installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Documenting authenticator types approved for use, the frequency for changing/refreshing, and the technical justification that demonstrates that adequate security is provided by the frequency;
- Protecting authenticator content from unauthorized disclosure and modification;
- Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- Changing authenticators for group/role accounts when membership to those accounts changes.

[Licensee/Applicant] requires that the registration process to receive authenticators be conducted in person or by a trusted third party with management authorization.

D-36 PASSWORD-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (1))

For password-based authentication for the VDA, the [Licensee/Applicant]:

- Enforces a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security;
- Enforces password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters;
- Enforces a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries;
- Stores and transmits only cryptographically-protected passwords;
- Enforces lifetime restrictions for password minimums of 1 day and provides a technical basis for maximums defined and documented by the CST that prevents unauthorized access;
- Prohibits password reuse for 10 generations;
- Requires an immediate change to a permanent password upon the first logon, when temporary passwords are used for VDA logons; and

- Stores written or electronic copies of master passwords in a secure location with limited access.

D-37 PUBLIC KEY INFRASTRUCTURE (PKI)-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (2))

[Licensee/Applicant] ensures that PKI-based authentication for the VDA:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group; and
- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

D-38 IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (3))

[Licensee/Applicant] requires that the registration process to receive authenticators be conducted in person or by a trusted third party with management authorization.

D-39 HARDWARE TOKEN-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (11))

[Licensee/Applicant] ensures that hardware token-based authentication for the VDA, employs mechanisms that satisfy Level 4 as described in NIST SP 800-63-2 or later revisions.

D-40 AUTHENTICATOR FEEDBACK
(Informed by NIST SP 800-53 Rev. 4, IA-6)

[Licensee/Applicant] ensures the VDA obscures feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

D-41 CRYPTOGRAPHIC MODULE AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-7)

[Licensee/Applicant] ensures the VDA implements mechanisms for authentication to a cryptographic module based on NIST Cryptographic Module Validation Program (CMVP) and associated guidance for such authentication.

D-42 INCIDENT RESPONSE TRAINING
(Informed by NIST SP 800-53 Rev. 4, IR-2, IR-2 (1), and IR-2 (2))

[Licensee/Applicant] provides incident response training to VDA users consistent with assigned roles and responsibilities:

- Within 92 days of assuming an incident response role or responsibility;
- When required by VDA changes; and
- At least every 12 months.

[Licensee/Applicant]:

- Incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations; and
- Employs automated mechanisms to provide a more thorough and realistic incident response training environment.

D-43 INCIDENT RESPONSE TESTING
(Informed by NIST SP 800-53 Rev. 4, IR-3 and IR-3 (2))

[Licensee/Applicant]:

- Tests the incident response capability for the VDA at least every 92 days using one or more of the following methods to determine the incident response effectiveness and documents the results of checklists, walk-through or tabletop exercises, and simulations (parallel/full interrupt);
- Tests the incident response capability for the VDA at least every 36 months using a comprehensive exercise; and
- Coordinates incident response testing with organizational elements responsible for related plans.

D-44 INCIDENT HANDLING
(Informed by NIST SP 800-53 Rev. 4, IR-4, IR-4 (1), and IR-4 (4))

[Licensee/Applicant]:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities;
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly;
- Employs automated mechanisms to support the incident handling process; and
- Correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

D-45 INCIDENT MONITORING
(Informed by NIST SP 800-53 Rev. 4, IR-5 and IR-5 (1))

[Licensee/Applicant]

- Tracks and documents VDA security incidents; and
- Employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

D-46 INCIDENT REPORTING
(Informed by NIST SP 800-53 Rev. 4, IR-6 and IR-6 (1))

[Licensee/Applicant]:

- Requires personnel to report suspected cyber security incidents to the CST upon discovery; and
- Employs automated mechanisms to assist in the reporting of security incidents.

D-47 INCIDENT RESPONSE ASSISTANCE
(Informed by NIST SP 800-53 Rev. 4, IR-7 and IR-7 (1))

[Licensee/Applicant]:

- Provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the VDA for the handling and reporting of security incidents; and
- Employs automated mechanisms to increase the availability of incident response-related information and support.

D-48 INFORMATION SPILLAGE RESPONSE
(Informed by NIST SP 800-53 Rev. 4, IR-9, IR-9 (1), IR-9 (2), IR-9 (3), and IR-9 (4))

[Licensee/Applicant]:

- Responds to information spills by:
  - Identifying the specific information involved in the VDA contamination;
  - Alerting the CST of the information spill using a method of communication not associated with the spill;
  - Isolating the contaminated VDA or system component;
  - Eradicating the information from the contaminated VDA or component;
  - Identifying other VDAs or system components that may have been subsequently contaminated;
  - Documenting the incident; and
- Assigns authorized personnel with responsibility for responding to information spills;
- Provides information spillage response training at least every 12 months;
- Implements procedures to ensure that corrective actions associated with information spills cannot result in consequence of concern; and
- Utilizes appropriate response procedures and safeguards for personnel exposed to information not within assigned access authorizations.

D-49 CONTROLLED MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-2 and MA-2 (2))

[Licensee/Applicant]:

- Performs and documents maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern;
- Reviews records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days;
- Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Requires that CST approve the removal of the VDA for off-site maintenance or repairs outside the licensees positive control;
- Sanitizes equipment to remove all information from associated media prior to removal for off-site maintenance or repairs outside the licensees positive control;
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions;
- Includes in records of maintenance and repairs on VDA components at a minimum: date, time, identification of those performing the maintenance, description of maintenance performed, and VDA components removed or replaced;
- Retains records for inspection by the NRC;

- Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
- Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

D-50 MAINTENANCE TOOLS
(Informed by NIST SP 800-53 Rev. 4, MA-3, MA-3 (1), and MA-3 (2), and MA-3 (3))

[Licensee/Applicant]:
- Approves, controls, and monitors VDA maintenance tools;
- Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications; and
- Checks media containing diagnostic and test programs for malicious code before the media are used in the VDA.

[Licensee/Applicant] prevents the unauthorized removal of maintenance equipment containing VDA information by:
- Verifying that there is no VDA information contained on the equipment;
- Sanitizing or destroying the equipment;
- Retaining the equipment within the facility; or
- Obtaining an exemption from the CST explicitly authorizing removal of the equipment from the facility.

D-51 NONLOCAL MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant]:
- Approves and monitors nonlocal maintenance and diagnostic activities;
- Documents and only allows the use of nonlocal maintenance and diagnostic tools for the VDA where those tools do not introduce vulnerabilities or lead to a consequence of concern (e.g., information systems that perform maintenance on VDAS are protected equivalent to the VDA.);
- Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
- Maintains records for nonlocal maintenance and diagnostic activities; and
- Terminates session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant]:
- Documents the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections; or
- Removes the component to be serviced from the VDA prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to VDA information) before removal from licensee facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the VDA.

D-52 MAINTENANCE PERSONNEL
(Informed by NIST SP 800-53 Rev. 4, MA-5 and MA-5 (1))

[Licensee/Applicant]:
- Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

- Ensures that unescorted personnel performing maintenance on the VDA have required access authorizations; and
- Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

[Licensee/Applicant]:

- Implements procedures for the use of maintenance personnel that lack appropriate security clearances that include the following requirements:
  - Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the VDA by approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
  - Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the VDA are sanitized and all nonvolatile storage media are removed or physically disconnected from the VDA and secured; and
- Develops and implements alternate security safeguards in the event a VDA component cannot be sanitized, removed, or disconnected from the VDA.

D-53 TIMELY MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-6)

[Licensee/Applicant] obtains maintenance support and/or spare parts for VDAs that must remain operational to prevent a consequence of concern.

D-54 MEDIA ACCESS
(Informed by NIST SP 800-53 Rev. 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media includes any active storage device, passive storage device, or passive media that:

- Contain information used to manage, configure, maintain, secure or operate the VDA; or
- Are used on the VDA for any purpose.

D-55 MEDIA MARKING
(Informed by NIST SP 800-53 Rev. 4, MP-3)

[Licensee/Applicant] marks VDA media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

D-56 MEDIA STORAGE
(Informed by NIST SP 800-53 Rev. 4, MP-4)

[Licensee/Applicant]:

- Physically controls and securely stores VDA media; and
- Protects VDA media until the media are destroyed or sanitized using approved equipment, techniques, and procedures that would prevent recovery of the data by an adversary.

D-57 MEDIA TRANSPORT
(Informed by NIST SP 800-53 Rev. 4, MP-5 and MP-5 (4))

[Licensee/Applicant]:

- Protects and controls VDA media during transport outside of controlled areas;
- Maintains accountability for VDA media during transport outside of controlled areas;
- Documents activities associated with the transport of VDA media;
- Restricts the activities associated with the transport of VDA media to authorized personnel; and
- Implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

D-58 MEDIA SANITIZATION
(Informed by NIST SP 800-53 Rev. 4, MP-6, MP-6 (1), MP-6 (2), and MP-6 (3))

[Licensee/Applicant]:

- Sanitizes VDA media prior to disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary;
- Reviews, approves, tracks, documents, and verifies media sanitization and disposal actions;
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information;
- Tests sanitization equipment and procedures at least every 12 months to verify that the intended sanitization is being achieved; and
- Applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the VDA.

D-59 MEDIA USE
(Informed by NIST SP 800-53 Rev. 4, MP-7 and MP-7 (1))

[Licensee/Applicant] prohibits the use of any media with a VDA, except specifically approved VDA media with an identifiable and verifiable owner.

D-60 MONITORING PHYSICAL ACCESS
(Informed by NIST SP 800-53 Rev. 4, PE-6)

[Licensee/Applicant]:

- Monitors physical access to the facility where the VDA resides to detect and respond to physical security incidents;
- Reviews physical access logs in a timely manner and upon occurrence of anomalous behavior;
- Coordinates results of reviews and investigations with the organizational incident response capability; and
- Monitors physical access to the VDA to detect unauthorized access in a timely manner.

D-61 VULNERABILITY SCANNING
(Informed by NIST SP 800-53 Rev. 4, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), and RA-5 (5))

[Licensee/Applicant]:

- Scans for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA, applications or both are identified and reported;

- Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures;
  - Measuring vulnerability impact; and
- Analyzes vulnerability scan reports and results from security control assessments;
- Addresses vulnerabilities in a timely and technically justified manner to prevent a consequence of concern;
- Shares information obtained from the vulnerability scanning process and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other VDAs (i.e., systemic weaknesses or deficiencies);
- Employs vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned;
- Updates the VDA vulnerabilities scanned prior to a new scan;
- Employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information VDA components scanned and vulnerabilities checked);
- Determines what information about the VDA is discoverable by adversaries and takes measures to address the associated potential cyber security issues; and
- Implements privileged access authorization to the VDA for vulnerability scanning activities.

D-62 EXTERNAL INFORMATION SYSTEM SERVICES
(Informed by NIST SP 800-53 Rev. 4, SA-9 and SA-9 (2))

[Licensee/Applicant]:

- Requires that providers of external information system services that interact with VDAs comply with information security requirements and address security controls for the associated consequence of concern;
- Defines and documents oversight and user roles and responsibilities with regard to external information system services;
- Employs automated mechanisms to monitor security control compliance by external service providers on an ongoing basis; and
- Requires providers of external information system services that interact with VDAs to identify the functions, ports, protocols, and other services required for the use of such services.

D-63 DEVELOPER CONFIGURATION MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SA-10)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to:

- Perform configuration management during the VDA, component, or service lifecycle;
- Document, manage, and control the integrity of changes to the VDA, component, or service;
- Implement only organization-approved changes to the VDA, component, or service;
- Document approved changes to the VDA, component, or service and the potential security impacts of such changes; and
- Track security flaws and flaw resolution within the VDA, component, or service and report findings to CST.

D-64 DEVELOPER SECURITY TESTING AND EVALUATION
(Informed by NIST SP 800-53 Rev. 4, SA-11)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to:

- Create and implement a security assessment plan;
- Perform comprehensive cyber security testing and evaluation;
- Produce evidence of the execution of the security assessment plan and the results of the security testing and evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing and evaluation.

D-65 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
(Informed by NIST SP 800-53 Rev. 4, SA-15)

[Licensee/Applicant]:

- Requires the developer of the VDA, VDA component, or VDA service to follow a documented development process that:
  - Explicitly addresses security requirements;
  - Identifies the standards and tools used in the development process;
  - Documents the specific tool options and tool configurations used in the development process; and
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy VDA security requirements.

D-66 DEVELOPER SECURITY ARCHITECTURE AND DESIGN
(Informed by NIST SP 800-53 Rev. 4, SA-17)

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service e to produce a design specification and security architecture that:

- Is consistent with and supportive of the licensee's security architecture;
- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

D-67 SYSTEM PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-2, SC-3, and SC-4)

[Licensee/Applicant]:

- Separates user functionality on the VDA (including user interface services) from VDA management functionality;
- Isolates security functions from nonsecurity functions on the VDA; and
- Prevents unauthorized and unintended information transfer via shared resources.

D-68 DENIAL OF SERVICE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-5)

[Licensee/Applicant] protects against or limits the effects of denial of service attacks by employing technical safeguards and countermeasures.

D-69 BOUNDARY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-7, SC-7 (3), SC-7 (4), SC-7 (5), and SC-7 (7))

[Licensee/Applicant] ensures the VDA:

- Monitors and controls communications at the boundary of the VDA and at key internal boundaries within the VDA;
- Implements subnetworks for publicly or externally accessible VDA components that are physically or logically separated from internal [licensee/applicant] networks; and
- Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security architecture.

D-70 EXTERNAL TELECOMMUNICATIONS SERVICES
(Informed by NIST SP 800-53 Rev. 4, SC-7 (4), SC-7 (5), SC-7 (7). SC-7 (8), SC-7 (10), SC-7 (11), SC-7 (12), SC-7 (14), SC-7 (18), SC-7 (20), and SC-7 (21))

[Licensee/Applicant]:

- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- Reviews exceptions to the traffic flow policy on a timely basis and removes exceptions that are no longer supported by an explicit mission/business need;
- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- Reviews exceptions to the traffic flow policy at least every 30 days and removes exceptions that are no longer supported by an explicit mission/business need;
- Prevents the unauthorized exfiltration of information across managed interfaces;
- Allows only incoming communications from authorized sources to be routed to VDAs;
- Implements host-based firewalls on VDAs;
- Protects against unauthorized physical connections to the VDA; and
- Employs boundary mechanisms.

[Licensee/Applicant] ensures the VDA:

- Has managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception);

- Prevents, in conjunction with a remote device, the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks;
- Routes internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
- Provides the capability to dynamically isolate/segregate VDAs from other VDAs; and
- Fails securely and safely in the event of an operational failure of a boundary protection device.

D-71 TRANSMISSION CONFIDENTIALITY AND INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures the VDA:

- Protects the confidentiality and integrity of transmitted information; and
- Implements cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to information during transmission, unless the transmission medium is otherwise protected by alternative physical safeguards.

D-72 NETWORK DISCONNECT
(Informed by NIST SP 800-53 Rev. 4, SC-10)

[Licensee/Applicant] terminates the network connection associated with a VDA communications session at the end of the session or within 10 minutes of inactivity, except for communications sessions that are necessary for safe operation of the VDA or are necessary to prevent a consequence of concern.

D-73 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SC-12 and SC-12 (1))

[Licensee/Applicant]:

- Establishes and manages cryptographic keys for required cryptography employed within the VDA in accordance with NIST CMVP; and
- Maintains availability of information necessary to safely operate the VDA or prevent a consequence of concern in the event of the loss of cryptographic keys by users.

D-74 COLLABORATIVE COMPUTING DEVICES
(Informed by NIST SP 800-53 Rev. 4, SC-15, SC-15 (1), SC-15 (3), and SC-15 (4))

[Licensee/Applicant] disables or removes collaborative computing devices from digital assets in areas where access could disclose information leading to a consequence of concern.

[Licensee/Applicant] ensures the VDA:

- Prohibits remote activation of collaborative computing devices except where explicitly authorized;
- Provides an explicit indication of use to users physically present at the devices;
- Provides physical disconnect of collaborative computing devices in a manner that supports ease of use; and
- Provides an explicit indication of current participants in collaborative sessions.

D-75 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
(Informed by NIST SP 800-53 Rev. 4, SC-17)

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

D-76 VOICE OVER INTERNET PROTOCOL (VOIP)
(Informed by NIST SP 800-53 Rev. 4, SC-19)

[Licensee/Applicant]:

- Establishes usage restrictions and implementation guidance VoIP technologies based on the potential to cause damage to the VDA if used maliciously; and
- Authorizes, monitors, and controls the use of VoIP within the VDA.

D-77 SECURE NAME / ADDRESS RESOLUTION
(Informed by NIST SP 800-53 Rev. 4, SC-20, SC-20a, SC-21, and SC-22)

[Licensee/Applicant] ensures the VDA:

- Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the VDA returns in response to external name/address resolution queries;
- Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace;
- Requests and performs data origin authentication and data integrity verification on the name/address resolution responses the VDA receives from authoritative sources; and
- Collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

D-78 SESSION AUTHENTICITY
(Informed by NIST SP 800-53 Rev. 4, SC-23)

[Licensee/Applicant] ensures the VDA protects the authenticity of communications sessions.

D-79 FAIL IN KNOWN STATE
(Informed by NIST SP 800-53 Rev. 4, SC-24)

[Licensee/Applicant]:

- Ensures VDAs fail in a known-state to ensure that functions are not adversely impacted; and
- Prevents a loss of confidentiality, integrity, or availability in the event of a failure of the VDA or a component of the VDA.

D-80 PROTECTION OF INFORMATION AT REST
(Informed by NIST SP 800-53 Rev. 4, SC-28)

[Licensee/Applicant] protects the confidentiality and integrity of VDA information at rest.

D-81 PROCESS ISOLATION
(Informed by NIST SP 800-53 Rev. 4, SC-39)

[Licensee/Applicant] maintains a separate execution domain for each executing process.

D-82 FLAW REMEDIATION
(Informed by NIST SP 800-53 Rev. 4, SI-2 and SI-2 (2))

[Licensee/Applicant]:

- Identifies, reports, and corrects VDA flaws;
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- Correcting the flaw expeditiously using the configuration management process;
- Incorporates flaw remediation into the organizational configuration management process;
- Performs vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production; and
- Employs automated mechanisms to determine the state of VDA components with regard to flaw remediation.

D-83 MALICIOUS CODE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-3, SI-3 (1), SI-3 (2), SI-3 (8), and SI-3 (10))

[Licensee/Applicant]:

- Employs malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code;
- Updates malicious code protection mechanisms whenever new releases are available;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the VDA at least every 7 days;
  - Perform real-time scans of files from external sources as the files are downloaded, opened, or executed;
  - Prevent malicious code execution;
  - Alert the CST of the detection of malicious code in a timely manner; and
- Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA;
- Centrally manages malicious code protection mechanisms;
- Automatically updates malicious code protection mechanisms for the VDA;
- Detects unauthorized operating system commands in VDAs through the kernel application programming interface and:
  - Issues a warning;
  - Audits the command execution;
  - Prevents the execution of the command; and
- Employs tools and techniques to analyze the characteristics and behavior of malicious code; and
- Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

D-84 VDA MONITORING
(Informed by NIST SP 800-53 Rev. 4, SI-4, SI-4 (2), SI-4 (4), and SI-4 (5))

[Licensee/Applicant]:

- Monitors the VDA to detect:

  - Cyber attacks and indicators of potential cyber attacks;
  - Unauthorized local, network, and remote connections; and
- Identifies unauthorized use of the VDA using automated or other means;
- Deploys monitoring devices:
  - Strategically within the VDA to collect organization-determined essential information;
  - At ad hoc locations within the system to track specific types of transactions of interest to the organization; and
- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- Heightens the level of VDA 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;
- Provides VDA monitoring information to appropriate licensee cyber security personnel as necessary;
- Employs automated tools to support near real-time analysis of events;
- Monitors inbound and outbound communications traffic for the VDA in near real-time for unusual or unauthorized activities or conditions; and
- Ensures appropriate cyber security personnel are alerted when indications of compromise or potential compromise of the VDA occurs.

D-85 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
(Informed by NIST SP 800-53 Rev. 4, SI-5 and SI-5 (1))

[Licensee/Applicant]:

- Receives cyber security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis;
- Generates internal security alerts, advisories, and directives as necessary to prevent a consequence of concern;
- Disseminates security alerts, advisories, and directives to appropriate personnel and the NRC;
- Implements security directives in a timely manner; and
- Employs automated mechanisms to make security alert and advisory information available throughout the organization.

D-86 SECURITY FUNCTION VERIFICATION
(Informed by NIST SP 800-53 Rev. 4, SI-6 and SI-6 (3))

[Licensee/Applicant]:

- Verifies the correct operation of security functions;
- Performs this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and when anomalies are discovered;
- Notifies appropriate personnel in a timely manner of failed security verification tests; and
- Reports the results of security function verification to the CST.

D-87 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SI-7, SI-7 (1), SI-7 (2), SI-7 (5), SI-7 (7), SI-7 (12), SI-7 (12), SI-7 (14))

[Licensee/Applicant]:

- Employs integrity verification tools to detect unauthorized changes to VDA software, firmware, and information;

- Performs an integrity check of VDA software, firmware, and information. This occurs, where possible, upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and when anomalies are discovered;
- Employs automated tools that provide notification to appropriate personnel upon discovering discrepancies during integrity verification;
- Automatically takes proactive protection measures when VDA integrity violations are discovered;
- Incorporates the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability;
- Requires that the integrity of software be verified prior to execution; and
- Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.

D-88 ENHANCEMENTS TO INFORMATION INPUT VALIDATION
(Informed by NIST SP 800-53 Rev. 4, SI-10 (5))

[Licensee/Applicant] restricts the use of information inputs to defined trusted sources and defined formats.

D-89 ERROR HANDLING
(Informed by NIST SP 800-53 Rev. 4, SI-11)

[Licensee/Applicant] ensures the VDA:
- Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- Reveals error messages only to authorized personnel with a need-to-know.

D-90 INFORMATION HANDLING AND RETENTION
(Informed by NIST SP 800-53 Rev. 4, SI-12)

[Licensee/Applicant] handles and retains information within the VDA and information output from the VDA in accordance with NRC record retention requirements.

D-91 MEMORY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-16)

[Licensee/Applicant] implements automated mechanisms and safeguards for the VDA to protect its memory from unauthorized code execution.

APPENDIX E

ADDITIONAL CYBER SECURITY CONTROLS FOR VITAL DIGITAL ASSETS ASSOCIATED WITH ACTIVE CONSEQUENCES OF CONCERN – SAFETY

E-1 ACCOUNT MANAGEMENT PROCEDURES

(Informed by National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, AC-2)

[Licensee/Applicant] employs, at a minimum, the following measures in support of the management of user accounts on vital digital assets (VDAs):

- Assigns account managers for VDA accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires independent management approval for requests to create VDA accounts;
- Creates, enables, modifies, disables, and removes VDA accounts in accordance with the Access Control policy;
- Monitors the use of VDA accounts;
- Notifies account managers in a timely manner:
  - When accounts are no longer required;
  - When users are terminated or transferred;
  - When individual VDA usage or need-to-know changes; and
- Authorizes access to the VDA based on:
  - A valid access authorization;
  - Intended VDA usage; and
- Reviews accounts at least every 30 days for compliance with account management requirements; and
- Employs, at a minimum, the following measures to restrict the creation and issuance of shared/group VDA accounts:
  - Ensures shared/group account requests:
    - Are issued only when necessary to prevent a consequence of concern;
    - Include a documented technical justification;
    - Are reviewed and approved by the Cyber Security Team (CST) prior to issuance; and
  - Automatically terminates and establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

E-2 ACCOUNT MANAGEMENT

(Informed by NIST SP 800-53 Rev. 4, AC-2 (5), AC-2 (12), and AC-2 (13))

[Licensee/Applicant] employs, at minimum, the following measures in support of the management of VDA accounts using a combination of procedural activity and automated means:

- Requires that users log out within 15 minutes of inactivity unless the login session must be maintained to prevent a consequence of concern;
- Monitors VDA accounts for atypical usage and anomalous activity that could indicate account compromise;
- Reports atypical usage of VDA accounts to the CST; and

- Disables user accounts that have been potentially compromised upon discovery.

E-3 AUTOMATED ACCOUNT MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-2 (1), AC-2 (2), AC-2 (3), and AC-2 (4))

[Licensee/Applicant] employs, at minimum, the following automated technical mechanisms to support the management of VDA accounts, including:

- Automatically removes or disables temporary and emergency accounts once they are no longer needed;
- Automatically disables inactive accounts within 30 days; and
- Automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate personnel in a timely manner.

E-4 ACCESS MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-3 and AC-4)

[Licensee/Applicant] ensures VDAs employ technical measures in support of the enforcement of account access to enforce approved authorizations for:

- Logical access to VDA information and VDA resources in accordance with applicable access control policies; and
- Controlling the flow of information within the VDA and between interconnected systems and VDAs.

E-5 REMOTE ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-17)

[Licensee/Applicant]:

- Establishes and documents usage restrictions, configurations, connection requirements, and implementation guidance for each type of remote access allowed; and
- Authorizes remote access to the VDA prior to allowing such connections.

E-6 MANAGED ACCESS CONTROL POINTS
(Informed by NIST SP 800-53 Rev. 4, AC-17 (3))

[Licensee/Applicant] ensures all remote accesses to VDAs is through a boundary control device meeting the requirements in cyber security control, "BOUNDARY PROTECTION," of this Appendix.

E-7 WIRELESS ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-18)

[Licensee/Applicant]:

- Establishes usage restrictions, configurations, connection requirements, and implementation guidance for wireless access; and
- Authorizes wireless access to the VDA prior to allowing such connections.

E-8 RESTRICT CONFIGURATIONS BY USERS
(Informed by NIST SP 800-53 Rev. 4, AC-18 (4))

[Licensee/Applicant] identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

E-9 ANTENNAS AND TRANSMISSION POWER LEVELS
(Informed by NIST SP 800-53 Rev. 4, AC-18 (5))

[Licensee/Applicant] selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be accessed outside of licensee-controlled boundaries.

E-10 EXTERNAL INFORMATION SHARING
(Informed by NIST SP 800-53 Rev. 4, AC-21)

When VDA information is shared with external parties, [licensee/applicant]:

- Ensures that access authorizations assigned to the sharing partner match the access restrictions on the information; and
- Employs automated mechanisms to enforce these restrictions.

E-11 USE OF EXTERNAL INFORMATION SYSTEMS
(Informed by NIST SP 800-53 Rev. 4, AC-20, AC-20 (1), and AC-20 (2))

[Licensee/Applicant] establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- Access the VDA from external information systems; and
- Process, store, or transmit organization-controlled information using external information systems.

[Licensee/Applicant]:

- Restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems; and
- Permits authorized individuals to use an external information system to access the VDA or to process, store, or transmit organization-controlled information only when the [licensee/applicant]:
  - Verifies the implementation of security controls on the external system equivalent to security controls addressed for the VDA; or
  - Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

E-12 AUDIT DATA DEFINITION, GENERATION, AND CONTENT
(Informed by NIST SP 800-53 Rev. 4, AU-3, AU-3 (1), AU-3 (2), AU-5, AU-5 (2), AU-12, AU-12 (3), AU-14, AU-14 (1), and AU-14 (2))

[Licensee/Applicant] ensures the VDA:

- Generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event; and
- Generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum:

- Account (user or service) login failure;
- Account role or privilege change;
- File or object creation, modification and deletion;
- Service start and stop;
- Privileged service call;
- Account creation and modification;
- Account right assignment;
- Audit policy change;
- User account password change;
- User group creation and modification; and
- Remote session start and failure.

[Licensee/Applicant] ensures the VDA auditing function:

- Alerts cyber security personnel in near real-time of an audit processing failure, or where audit failure events occur that could indicate VDA compromise;
- Takes automated measures to preserve audit data;
- Provides the capability to increase or modify audit record content in response to threat intelligence;
- Initiates session audits at VDA start-up;
- provides the capability for authorized users to select a user session to capture/record or view/hear;
- Provides the capability for authorized users to capture/record and log content related to a user session; and
- Provides centralized management and configuration of the content to be captured in audit records.

E-13 AUDIT DATA MANAGEMENT AND PROTECTION
(Informed by NIST SP 800-53 Rev. 4, AU-4, AU-5 (1), AU-9, AU-9 (2), AU-9 (3), AU-9 (4), and AU-10)

[Licensee/Applicant]:

- Allocates sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configures auditing to prevent capacity from being exceeded;
- Authorizes access to management of audit functionality to only authorized users with cyber security responsibilities;
- Ensures the VDA provides an alert to authorized personnel when allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity;
- Ensures the VDA backs up audit records onto a physically different VDA than the VDA being audited;
- Ensures the VDA protects audit information and audit tools from unauthorized access, modification, and deletion;
- Ensures the VDA implements cryptographic mechanisms to protect the integrity of audit information and audit tools; and
- Ensures the VDA protects against an individual (or process acting on behalf of an individual) falsely denying having performed any action on the VDA.

E-14 AUDIT REVIEW, ANALYSIS, AND REPORTING
(Informed by NIST SP 800-53 Rev. 4, AU-6, AU-6 (1), AU-6 (3), AU-6 (5), AU-6 (6), and AU-12 (1))

[Licensee/Applicant]:

- Employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities;
- Reviews and analyzes VDA audit records in a timely manner for indications of potential compromise;
- Analyzes and correlates audit records across different repositories to gain organization-wide situational awareness;
- Integrates analysis of audit records with analysis of vulnerability scanning information, performance data, VDA monitoring information, and data/information collected from other sources to further enhance the ability to identify potential unauthorized activity;
- Correlates information from audit records with information obtained from monitoring physical access to the VDA to further enhance the ability to identify potential unauthorized activity;
- Reports findings to the CST; and
- Ensures the VDA compiles audit records into a logical or physical audit trail that is time-correlated to, at a minimum, within one-tenth of a second.

E-15 SECURITY CONTROL ASSESSMENTS
(Informed by NIST SP 800-53 Rev. 4, CA-2 (2))

[Licensee/Applicant] includes and documents as part of VDA security control assessments:

- An attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
- Announced assessments:
  - In-depth monitoring (to be done automatically, in real time);
  - Vulnerability scanning (to be done at least every 30 days);
  - Malicious actor testing (to be done at least every 92 days); and
- Unannounced assessments (in addition to announced assessments above):
  - Vulnerability scanning (to be done at least every 183 days);
  - Malicious actor testing (to be done at least every 12 months); and
  - Performance/load testing (to be done at least every 183 days).

E-16 INDEPENDENCE OF ASSESSORS
(Informed by NIST SP 800-53 Rev. 4, CA-2 (1), CA-7 (1), CA-8, and CA-8 (1))

[Licensee/Applicant]:

- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to conduct assessments of the cyber security controls;
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to monitor the cyber security controls for the VDA on an ongoing basis;
- Conducts penetration testing at least every 12 months on the VDA; and
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to perform penetration testing on the VDA.

E-17 ENHANCEMENTS TO VDA CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant]:

- Employs a "deny-all, permit-by-exception" policy for allowing VDAs to connect to external information systems;
- Prohibits the direct connection of a VDA to an external network without the use of:
  - At least one separate, intervening access control device (e.g. firewall, cross domain solution);
  - At least one separate, intervening intrusion detection/prevention mechanism with near real-time prevention, detection and alerting capability;
  - Host-based protective measures;
  - Other measures necessary to prevent a consequence of concern; and
- Prohibits the direct connection of a VDA to a public network;
- Authorizes connections to the VDA; and
- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

E-18 AUTOMATED BASELINE CONFIGURATION
(Informed by NIST SP 800-53 Rev. 4, CM-2 (2))

[Licensee/Applicant] employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the VDA.

E-19 CONFIGURE VDAS FOR HIGH-RISK AREAS
(Informed by NIST SP 800-53 Rev. 4, CM-2 (7))

Prior to transporting VDAs associated with an active consequence of concern to locations that the [licensee/applicant] deems to be of significant risk, the [licensee/applicant]:

- Documents a detailed justification for the VDA to be transported;
- Obtains written approval from the CST and management;
- Documents the VDA configuration baseline and component inventory prior to leaving controlled areas;
- Observes chain-of-custody of the VDA or VDA component;
- Performs a review of the VDA configuration baseline and component inventory upon return;
- Performs testing of the VDA to ensure no cyber compromise has occurred; and
- Performs a security control assessment to ensure all controls are in place, operational, and performing the intended function.

E-20 CONFIGURATION CHANGE CONTROL
(Informed by NIST SP 800-53 Rev. 4, CM-3)

[Licensee/Applicant]:

- Documents changes to the VDA that will be configuration-controlled per Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53;
- Reviews proposed configuration-controlled changes to the VDA and approves or disapproves such changes with explicit consideration for security impact analyses before implementation of the change;
- Documents configuration change decisions associated with the VDA;
- Implements approved configuration-controlled changes to the VDA;

- Retains records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements;
- Audits and reviews activities associated with configuration-controlled changes to the VDA; and
- Coordinates and provides oversight for configuration change control activities through the change management process.

E-21 CHANGE TESTING AND ANALYSIS
(Informed by NIST SP 800-53 Rev. 4, CM-3 (2), CM-4, and CM-4 (1))

[Licensee/Applicant]:

- Tests, validates, and documents changes to the VDA before implementing the changes to the VDA;
- Analyzes changes to the VDA to determine potential security impacts prior to change implementation; and
- Analyzes changes to the VDA in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

E-22 ACCESS RESTRICTIONS FOR CHANGE
(Informed by NIST SP 800-53 Rev. 4, CM-5 and CM-5 (1))

[Licensee/Applicant]:

- Defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the VDA; and
- Ensures VDA enforces access restrictions and supports auditing of the enforcement actions.

E-23 REVIEW VDA CHANGES
(Informed by NIST SP 800-53 Rev. 4, CM-5 (2))

[Licensee/Applicant] reviews VDA changes at least every 183 days or in the event of suspected compromise to determine whether unauthorized changes have occurred.

E-24 SIGNED COMPONENTS
(Informed by NIST SP 800-53 Rev. 4, CM-5 (3))

[Licensee/Applicant] ensures the VDA prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

E-25 CONFIGURATION SETTINGS
(Informed by NIST SP 800-53 Rev. 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant]:

- Establishes and documents configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves any deviations from established configuration settings;
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;

- Employs automated mechanisms to centrally manage, apply, and verify VDA configuration settings; and
- Reports unauthorized changes to VDA configuration settings to the cyber security incident response team upon detection.

E-26 LEAST FUNCTIONALITY
(Informed by NIST SP 800-53 Rev. 4, CM-7)

[Licensee/Applicant]:
- Configures the VDA to provide only essential capabilities, to perform its function and maintain safe and secure operations; and
- Prohibits or restricts the use of unneeded functions, ports, protocols, and/or services.

E-27 PERIODIC REVIEW
(Informed by NIST SP 800-53 Rev. 4, CM-7 (1))

[Licensee/Applicant]:
- Reviews the VDA at least every 30 days to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
- Disables or restricts unneeded functions, ports, protocols, and/or services identified by the review.

E-28 AUTHORIZED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-7 (2) and CM-7 (4))

[Licensee/Applicant]:
- Identifies software programs authorized to execute on the VDA;
- Employs an "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA;
- Reviews and updates the list of authorized software programs, at least every 183 days; and
- Employs automated mechanisms for the VDA (i.e. application white-listing) to prevent unauthorized program execution.

E-29 VDA COMPONENT INVENTORY
(Informed by NIST SP 800-53 Rev. 4, CM-8, CM-8 (1), CM-8 (2), CM-8 (3), and CM-8 (4)

[Licensee/Applicant]:
- Develops and documents an inventory of VDA components that:
  - Accurately reflects the current VDA;
  - Includes all components within the boundary of the VDA;
  - Is at the level of granularity necessary for tracking and reporting;
  - Includes information necessary to achieve effective VDA component accountability; and
- Reviews and updates the VDA component inventory at least every 92 days or as part of any changes to a VDA;
- Updates the inventory of VDA components as an integral part of component installations, removals, and VDA updates;
- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA;
- Employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components;

- Includes in the VDA component inventory information, a means for identifying individuals responsible/accountable for administering those components; and
- Takes appropriate actions when unauthorized components are detected to remove, disable, or otherwise prevent the unauthorized component from causing a consequence of concern.

E-30 INSTALLED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-11)

[Licensee/Applicant]:
- Establishes policies governing the installation of software on VDAs consistent with configuration management in 10 CFR 73.53(f);
- Enforces software installation policies using automated measures where supported; and
- Monitors policy compliance using automated measures where supported.

E-31 IDENTIFICATION AND AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-2, IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (8), IA-2 (9), IA-2 (11), IA-2 (12), IA-3, and IA-8)

[Licensee/Applicant] ensures the VDA:
- Uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and non-organizational users (or processes acting on behalf of non-organizational users);
- Implements multifactor authentication for network access to privileged accounts;
- Implements multifactor authentication for network access to non-privileged accounts;
- Implements multifactor authentication for local access to privileged accounts;
- Implements multifactor authentication for local access to non-privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to non-privileged accounts;
- Implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the VDA gaining access and the device meets E-authentication Assurance Level 3 as described in NIST SP 800-63-2 or later revisions;
- Accepts and electronically verifies Personal Identity Verification credentials; and
- Uniquely identifies and authenticates devices before establishing a connection to a VDA.

E-32 IDENTIFIER MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-4)

[Licensee/Applicant] manages VDA identifiers by:
- Receiving independent management authorization to assign an individual, group, role, or device identifier;
- Selecting an identifier that identifies an individual, group, role, or device;
- Assigning the identifier to the intended individual, group, role, or device;
- Preventing reuse of identifiers where reuse could allow unintended or unauthorized access; and
- Disabling the identifier within 30 days of inactivity.

E-33 AUTHENTICATOR MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the organization;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators prior to VDA installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Documenting authenticator types approved for use, the frequency for changing/refreshing, and the technical justification that demonstrates that adequate security is provided by the frequency;
- Protecting authenticator content from unauthorized disclosure and modification;
- Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- Changing authenticators for group/role accounts when membership to those accounts changes.

[Licensee/Applicant] requires that the registration process to receive authenticators be conducted in person or by a trusted third party with management authorization.

E-34 PASSWORD-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (1))

For password-based authentication for the VDA, the [Licensee/Applicant]:

- Enforces a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security;
- Enforces password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters;
- Enforces a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries;
- Stores and transmits only cryptographically-protected passwords;
- Enforces lifetime restrictions for password minimums of 1 day and provides a technical basis for maximums defined and documented by the CST that prevents unauthorized access;
- Prohibits password reuse for 10 generations;
- Requires an immediate change to a permanent password upon the first logon, when temporary passwords are used for VDA logons; and
- Stores written or electronic copies of master passwords in a secure location with limited access.

E-35 PUBLIC KEY INFRASTRUCTURE (PKI)-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (2))

[Licensee/Applicant] ensures that PKI-based authentication for the VDA:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group; and

- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

E-36 HARDWARE TOKEN-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (11))

[Licensee/Applicant] ensures that the VDA, for hardware token-based authentication, employs mechanisms that satisfy E-authentication Assurance Level 3 as described in NIST SP 800-63-2 or later revisions.

E-37 AUTHENTICATOR FEEDBACK
(Informed by NIST SP 800-53 Rev. 4, IA-6)

[Licensee/Applicant] ensures that the VDA obscures feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

E-38 CRYPTOGRAPHIC MODULE AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-7)

[Licensee/Applicant] ensures that the VDA implements mechanisms for authentication to a cryptographic module based on NIST Cryptographic Module Validation Program (CMVP) and associated guidance for such authentication.

E-39 INCIDENT RESPONSE TRAINING
(Informed by NIST SP 800-53 Rev. 4, IR-2, IR-2 (1), and IR-2 (2))

[Licensee/Applicant] provides incident response training to VDA users consistent with assigned roles and responsibilities:

- Within 92 days of assuming an incident response role or responsibility;
- When required by VDA changes; and
- At least every 12 months.

[Licensee/Applicant]:

- Incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations; and
- Employs automated mechanisms to provide a more thorough and realistic incident response training environment.

E-40 INCIDENT RESPONSE TESTING
(Informed by NIST SP 800-53 Rev. 4, IR-3 and IR-3 (2))

[Licensee/Applicant]:

- Tests the incident response capability for the VDA at least every 92 days using one or more of the following methods to determine the incident response effectiveness and documents the results of checklists, walk-through or tabletop exercises, and simulations (parallel/full interrupt);
- Tests the incident response capability for the VDA at least every 36 months using a comprehensive exercise; and
- Coordinates incident response testing with organizational elements responsible for related plans.

E-41 INCIDENT HANDLING
(Informed by NIST SP 800-53 Rev. 4, IR-4, IR-4 (1), and IR-4 (4))

[Licensee/Applicant]:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities;
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly;
- Employs automated mechanisms to support the incident handling process; and
- Correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

E-42 INCIDENT MONITORING
(Informed by NIST SP 800-53 Rev. 4, IR-5 and IR-5 (1))

[Licensee/Applicant]

- Tracks and documents VDA security incidents; and
- Employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

E-43 INCIDENT REPORTING
(Informed by NIST SP 800-53 Rev. 4, IR-6 and IR-6 (1))

[Licensee/Applicant]:

- Requires personnel to report suspected cyber security incidents to the CST upon discovery; and
- Employs automated mechanisms to assist in the reporting of security incidents.

E-44 INCIDENT RESPONSE ASSISTANCE
(Informed by NIST SP 800-53 Rev. 4, IR-7, IR-7 (1), and IR-7 (2))

[Licensee/Applicant]:

- Provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the VDA for the handling and reporting of security incidents; and
- Employs automated mechanisms to increase the availability of incident response-related information and support.

[Licensee/Applicant]:

- Establishes a direct, cooperative relationship between its incident response capability and external providers of cyber security protection capabilities; and
- Identifies organizational cyber security incident response team members to the external providers.

E-45 CONTROLLED MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-2 and MA-2 (2))

[Licensee/Applicant]:

- Performs and documents maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern;

- Reviews records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days;
- Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Requires that CST approve the removal of the VDA for off-site maintenance or repairs outside the licensees positive control;
- Sanitizes equipment to remove all information from associated media prior to removal for off-site maintenance or repairs outside the licensees positive control;
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions;
- Includes in records of maintenance and repairs on VDA components at a minimum: date, time, identification of those performing the maintenance, description of maintenance performed, and VDA components removed or replaced;
- Retains records for inspection by the NRC;
- Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
- Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

E-46 MAINTENANCE TOOLS
(Informed by NIST SP 800-53 Rev. 4, MA-3, MA-3 (1), and MA-3 (2))

[Licensee/Applicant]:

- Approves, controls, and monitors VDA maintenance tools;
- Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications; and
- Checks media containing diagnostic and test programs for malicious code before the media are used in the VDA.

[Licensee/Applicant] prevents the unauthorized removal of maintenance equipment containing VDA information by:

- Verifying that there is no VDA information contained on the equipment;
- Sanitizing or destroying the equipment;
- Retaining the equipment within the facility; or
- Obtaining an exemption from the CST explicitly authorizing removal of the equipment from the facility.

E-47 NONLOCAL MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant]:

- Approves and monitors nonlocal maintenance and diagnostic activities;
- Documents and only allows the use of nonlocal maintenance and diagnostic tools for the VDA where those tools do not introduce vulnerabilities or lead to a consequence of concern (e.g., information systems that perform maintenance on VDAS are protected equivalent to the VDA.);
- Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
- Maintains records for nonlocal maintenance and diagnostic activities; and
- Terminates session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant]:

- Documents the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections; or
- Removes the component to be serviced from the VDA prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to VDA information) before removal from licensee facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the VDA.

E-48 MAINTENANCE PERSONNEL

(Informed by NIST SP 800-53 Rev. 4, MA-5 and MA-5 (1))

[Licensee/Applicant]:

- Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- Ensures that unescorted personnel performing maintenance on the VDA have required access authorizations; and
- Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

[Licensee/Applicant]:

- Implements procedures for the use of maintenance personnel that lack appropriate security clearances that include the following requirements:
  - Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the VDA by approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
  - Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the VDA are sanitized and all nonvolatile storage media are removed or physically disconnected from the VDA and secured; and
- Develops and implements alternate security safeguards in the event a VDA component cannot be sanitized, removed, or disconnected from the VDA.

E-49 TIMELY MAINTENANCE

(Informed by NIST SP 800-53 Rev. 4, MA-6)

[Licensee/Applicant] obtains maintenance support and/or spare parts for VDAs that must remain operational to prevent a consequence of concern.

E-50 MEDIA ACCESS

(Informed by NIST SP 800-53 Rev. 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media includes any active storage device, passive storage device or passive media that:

- Contain information used to manage, configure, maintain, secure or operate the VDA; or
- Are used on the VDA for any purpose.

E-51 MEDIA MARKING
(Informed by NIST SP 800-53 Rev. 4, MP-3)

[Licensee/Applicant] marks VDA media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

E-52 MEDIA STORAGE
(Informed by NIST SP 800-53 Rev. 4, MP-4)

[Licensee/Applicant]:

- Physically controls and securely stores VDA media; and
- Protects VDA media until the media are destroyed or sanitized using approved equipment, techniques, and procedures that would prevent recovery of the data by an adversary.

E-53 MEDIA TRANSPORT
(Informed by NIST SP 800-53 Rev. 4, MP-5 and MP-5 (4))

[Licensee/Applicant]:

- Protects and controls VDA media during transport outside of controlled areas;
- Maintains accountability for VDA media during transport outside of controlled areas;
- Documents activities associated with the transport of VDA media;
- Restricts the activities associated with the transport of VDA media to authorized personnel; and
- Implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

E-54 MEDIA SANITIZATION
(Informed by NIST SP 800-53 Rev. 4, MP-6, MP-6 (1), MP-6 (2), and MP-6 (3))

[Licensee/Applicant]:

- Sanitizes VDA media prior to disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary;
- Reviews, approves, tracks, documents, and verifies media sanitization and disposal actions;
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information;
- Tests sanitization equipment and procedures at least every 12 months to verify that the intended sanitization is being achieved; and
- Applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the VDA.

E-55 MEDIA USE
(Informed by NIST SP 800-53 Rev. 4, MP-7 and MP-7 (1))

[Licensee/Applicant] prohibits the use of any media with a VDA, except specifically approved VDA media with an identifiable and verifiable owner.

E-56 MONITORING PHYSICAL ACCESS
(Informed by NIST SP 800-53 Rev. 4, PE-6)

[Licensee/Applicant]:

- Monitors physical access to the facility where the VDA resides to detect and respond to physical security incidents;
- Reviews physical access logs in a timely manner and upon occurrence of anomalous behavior; and
- Coordinates results of reviews and investigations with the organizational incident response capability.

E-57 VULNERABILITY SCANNING
(Informed by NIST SP 800-53 Rev. 4, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), and RA-5 (5))

[Licensee/Applicant]:

- Scans for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA, applications or both are identified and reported;
- Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures;
  - Measuring vulnerability impact; and
- Analyzes vulnerability scan reports and results from security control assessments;
- Addresses vulnerabilities in a timely and technically justified manner to prevent a consequence of concern;
- Shares information obtained from the vulnerability scanning process and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other VDAs (i.e., systemic weaknesses or deficiencies);
- Employs vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned;
- Updates the VDA vulnerabilities scanned prior to a new scan;
- Employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information VDA components scanned and vulnerabilities checked);
- Determines what information about the VDA is discoverable by adversaries and takes measures to address the associated potential cyber security issues; and
- Implements privileged access authorization to the VDA for vulnerability scanning activities.

E-58 EXTERNAL INFORMATION SYSTEM SERVICES
(Informed by NIST SP 800-53 Rev. 4, SA-9 and SA-9 (2))

[Licensee/Applicant]:

- Requires that providers of external information system services that interact with VDAs comply with information security requirements and address security controls for the associated consequence of concern;
- Defines and documents oversight and user roles and responsibilities with regard to external information system services;
- Employs automated mechanisms to monitor security control compliance by external service providers on an ongoing basis; and

- Requires providers of external information system services that interact with VDAs to identify the functions, ports, protocols, and other services required for the use of such services.

E-59 DEVELOPER CONFIGURATION MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SA-10)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to:

- Perform configuration management during the VDA, component, or service lifecycle;
- Document, manage, and control the integrity of changes to the VDA, component, or service;
- Implement only organization-approved changes to the VDA, component, or service;
- Document approved changes to the VDA, component, or service and the potential security impacts of such changes; and
- Track security flaws and flaw resolution within the VDA, component, or service and report findings to CST.

E-60 DEVELOPER SECURITY TESTING AND EVALUATION
(Informed by NIST SP 800-53 Rev. 4, SA-11)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to:

- Create and implement a security assessment plan;
- Perform comprehensive cyber security testing and evaluation;
- Produce evidence of the execution of the security assessment plan and the results of the security testing and evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing/evaluation.

E-61 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
(Informed by NIST SP 800-53 Rev. 4, SA-15)

[Licensee/Applicant]:

- Requires the developer of the VDA, VDA component, or VDA service to follow a documented development process that:
  - Explicitly addresses security requirements;
  - Identifies the standards and tools used in the development process;
  - Documents the specific tool options and tool configurations used in the development process; and
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy VDA security requirements.

E-62 DEVELOPER SECURITY ARCHITECTURE AND DESIGN
(Informed by NIST SP 800-53 Rev. 4, SA-17)

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service e to produce a design specification and security architecture that:

- Is consistent with and supportive of the licensee's security architecture;

- Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

E-63 SYSTEM PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-2, SC-3, and SC-4)

[Licensee/Applicant]:
- Separates user functionality on the VDA (including user interface services) from VDA management functionality;
- Isolates security functions from nonsecurity functions on the VDA; and
- Prevents unauthorized and unintended information transfer via shared resources.

E-64 DENIAL OF SERVICE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-5)

[Licensee/Applicant] protects against or limits the effects of denial of service attacks by employing technical safeguards and countermeasures.

E-65 BOUNDARY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-7, SC-7 (3), SC-7 (4), SC-7 (5), SC-7 (7), SC-7 (8), SC-7 (14), SC-7 (18), and SC-7 (21))

[Licensee/Applicant]:
- Monitors and controls communications at the boundary of the VDA and at key internal boundaries within the VDA;
- Implements subnetworks for publicly or externally accessible VDA components that are physically or logically separated from internal [licensee/applicant] networks;
- Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security architecture; and
- Limits the number of external network connections to the VDA.

E-66 TRANSMISSION CONFIDENTIALITY AND INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures the VDA:
- Protects the confidentiality and integrity of transmitted information; and
- Implements cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to information during transmission, unless the transmission medium is otherwise protected by alternative physical safeguards.

E-67 NETWORK DISCONNECT
(Informed by NIST SP 800-53 Rev. 4, SC-10)

[Licensee/Applicant] terminates the network connection associated with VDA communications session at the end of the session or within 10 minutes of inactivity, except for communications sessions that are necessary for safe operation of the VDA or are necessary to prevent a consequence of concern.

E-68 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SC-12 and SC-12 (1))

[Licensee/Applicant]:

- Establishes and manages cryptographic keys for required cryptography employed within the VDA in accordance with NIST CMVP; and
- Maintains availability of information necessary to safely operate the VDA or prevent a consequence of concern in the event of the loss of cryptographic keys by users.

E-69 COLLABORATIVE COMPUTING DEVICES
(Informed by NIST SP 800-53 Rev. 4, SC-15, SC-15 (1), SC-15 (3), and SC-15 (4))

[Licensee/Applicant] disables or removes collaborative computing devices from digital assets in areas where access could disclose information leading to a consequence of concern.

[Licensee/Applicant] ensures the VDA:

- Prohibits remote activation of collaborative computing devices except where explicitly authorized;
- Provides an explicit indication of use to users physically present at the devices;
- Provides physical disconnect of collaborative computing devices in a manner that supports ease of use; and
- Provides an explicit indication of current participants in collaborative sessions.

E-70 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
(Informed by NIST SP 800-53 Rev. 4, SC-17)

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

E-71 VOICE OVER INTERNET PROTOCOL (VOIP)
(Informed by NIST SP 800-53 Rev. 4, SC-19)

[Licensee/Applicant]:

- Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the VDA if used maliciously; and
- Authorizes, monitors, and controls the use of VoIP within the VDA.

E-72 SECURE NAME / ADDRESS RESOLUTION
(Informed by NIST SP 800-53 Rev. 4, SC-20, SC-20a, SC-21, and SC-22)

[Licensee/Applicant] ensures the VDA:

- Provides additional data origin authentication and integrity verification artifacts for the VDA along with the authoritative name resolution data the VDA returns in response to external name/address resolution queries;
- Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace;
- Requests and performs data origin authentication and data integrity verification on the name/address resolution responses the VDA receives from authoritative sources; and

- Collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

E-73 SESSION AUTHENTICITY
(Informed by NIST SP 800-53 Rev. 4, SC-23)

[Licensee/Applicant] ensures the VDA protects the authenticity of communications sessions.

E-74 FAIL IN KNOWN STATE
(Informed by NIST SP 800-53 Rev. 4, SC-24)

[Licensee/Applicant]:
- Ensures VDAs fail in a known-state to ensure that functions are not adversely impacted; and
- Prevents a loss of confidentiality, integrity, or availability in the event of a failure of the VDA or a component of the VDA.

E-75 PROTECTION OF INFORMATION AT REST
(Informed by NIST SP 800-53 Rev. 4, SC-28)

[Licensee/Applicant] protects the confidentiality and integrity of VDA information at rest.

E-76 PROCESS ISOLATION
(Informed by NIST SP 800-53 Rev. 4, SC-39)

[Licensee/Applicant] maintains a separate execution domain for each executing process.

E-77 FLAW REMEDIATION
(Informed by NIST SP 800-53 Rev. 4, SI-2, SI-2 (1) and SI-2 (2))

[Licensee/Applicant]:
- Identifies, reports, and corrects VDA flaws;
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- Correcting the flaw expeditiously using the configuration management process;
- Incorporates flaw remediation into the organizational configuration management process;
- Performs vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production;
- Centrally manages the flaw remediation process; and
- Employs automated mechanisms to determine the state of VDA components with regard to flaw remediation.

E-78 MALICIOUS CODE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-3, SI-3 (1), SI-3 (2), SI-3 (8), and SI-2 (10))

[Licensee/Applicant]:
- Employs malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code;
- Updates malicious code protection mechanisms whenever new releases are available;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the VDA at least every 7 days;

  - Perform real-time scans of files from external sources as the files are downloaded, opened, or executed;
  - Prevent malicious code execution;
  - Alert the CST of the detection of malicious code in a timely manner; and
- Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA;
- Centrally manages malicious code protection mechanisms;
- Automatically updates malicious code protection mechanisms for the VDA;
- Detects unauthorized operating system commands in VDAs through the kernel application programming interface and:
  - Issues a warning;
  - Audits the command execution;
  - Prevents the execution of the command; and
- Employs tools and techniques to analyze the characteristics and behavior of malicious code; and
- Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

E-79 VDA MONITORING

(Informed by NIST SP 800-53 Rev. 4, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-4 (10), SI-4 (11), and SI-4 (20))

[Licensee/Applicant]:

- Monitors the VDA to detect:
  - Cyber attacks and indicators of potential cyber attacks;
  - Unauthorized local, network, and remote connections; and
- Identifies unauthorized use of the VDA using automated or other means;
- Deploys monitoring devices:
  - Strategically within the VDA to collect organization-determined essential information;
  - At ad hoc locations within the system to track specific types of transactions of interest to the organization; and
- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- Heightens the level of VDA 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;
- Provides VDA monitoring information to appropriate licensee cyber security personnel as necessary;
- Employs automated tools to support near real-time analysis of events;
- Monitors inbound and outbound communications traffic for the VDA in near real-time for unusual or unauthorized activities or conditions;
- Ensures appropriate cyber security personnel are notified when indications of compromise or potential compromise of the VDA occurs;
- Makes provisions so that encrypted communications traffic is visible to authorized network monitoring tools;
- Analyzes outbound communications traffic at the external boundary of the VDA and selected interior points within the VDA to discover anomalies; and
- Implements additional monitoring of privileged users.

E-80 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
(Informed by NIST SP 800-53 Rev. 4, SI-5 and SI-5 (1))

[Licensee/Applicant]:

- Receives security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis;
- Generates internal security alerts, advisories, and directives as necessary to prevent a consequence of concern;
- Disseminates security alerts, advisories, and directives to appropriate personnel and the NRC;
- Implements security directives in a timely manner; and
- Employs automated mechanisms to make security alert and advisory information available throughout the organization.

E-81 SECURITY FUNCTION VERIFICATION
(Informed by NIST SP 800-53 Rev. 4, SI-6 and SI-6 (3))

[Licensee/Applicant]:

- Verifies the correct operation of security functions;
- Performs this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and when anomalies are discovered; and
- Notifies appropriate personnel in a timely manner of failed security verification tests.

[Licensee/Applicant] reports the results of security function verification to the CST.

E-82 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SI-7, SI-7 (1), SI-7 (2), SI-7 (5), SI-7 (7), SI-7 (12), SI-7 (12), SI-7 (14))

[Licensee/Applicant]:

- Employs integrity verification tools to detect unauthorized changes to VDA software, firmware, and information;
- Performs an integrity check of VDA software, firmware, and information. This occurs, where possible, upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and when anomalies are discovered;
- Employs automated tools that provide notification to appropriate personnel upon discovering discrepancies during integrity verification;
- Automatically takes proactive protection measures when VDA integrity violations are discovered;
- Incorporates the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability;
- Requires that the integrity of software be verified prior to execution; and
- Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.

E-83 ERROR HANDLING
(Informed by NIST SP 800-53 Rev. 4, SI-11)

[Licensee/Applicant] ensures the VDA:

- Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- Reveals VDA error messages only to authorized personnel with a need-to-know.

E-84 INFORMATION HANDLING AND RETENTION
(Informed by NIST SP 800-53 Rev. 4, SI-12)

[Licensee/Applicant] handles and retains information within the VDA and information output from the VDA in accordance with NRC record retention requirements.

E-85 MEMORY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-16)

[Licensee/Applicant] implements automated mechanisms and safeguards for the VDA to protect its memory from unauthorized code execution.

APPENDIX F

ADDITIONAL CYBER SECURITY CONTROLS FOR VITAL DIGITAL ASSETS ASSOCIATED WITH LATENT CONSEQUENCES OF CONCERN – SAFETY and SECURITY

F-1 ACCOUNT MANAGEMENT PROCEDURES

(Informed by National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, AC-2)

[Licensee/Applicant] employs, at minimum, the following measures in support of the management of user accounts on vital digital assets (VDAs):

- Assigns account managers for VDA accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires independent management approval for requests to create VDA accounts;
- Creates, enables, modifies, disables, and removes VDA accounts in accordance with the Access Control policy;
- Monitors the use of VDA accounts;
- Notifies account managers in a timely manner:
  - When accounts are no longer required;
  - When users are terminated or transferred;
  - When individual VDA usage or need-to-know changes; and
- Authorizes access to the VDA based on:
  - A valid access authorization;
  - Intended VDA usage; and
- Reviews accounts at least every 30 days for compliance with account management requirements; and
- Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

F-2 ACCOUNT MANAGEMENT

(Informed by NIST SP 800-53 Rev. 4, AC-2 (5), AC-2 (12), and AC-2 (13))

[Licensee/Applicant] employs, at minimum, the following measures in support of the management of VDA accounts using a combination of procedural activity and automated means:

- Requires that users log out within 15 minutes of inactivity unless the login session must be maintained to prevent a consequence of concern.
- Monitors VDA accounts for atypical usage and anomalous activity that could indicate account compromise;
- Reports atypical usage of VDA accounts to the CST; and
- Disables user accounts that have been potentially compromised upon discovery.

F-3 AUTOMATED ACCOUNT MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-2 (1), AC-2 (2), AC-2 (3), and AC-2 (4))

[Licensee/Applicant] employs, at minimum, the following automated technical mechanisms to support the management of VDA accounts, including:

- Automatically removes or disables temporary and emergency accounts once they are no longer needed;
- Automatically disables inactive accounts within 30 days; and
- Automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate personnel in a timely manner.

F-4 ACCESS MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, AC-3 and AC-4)

[Licensee/Applicant] ensures the VDA employs technical measures in support of the enforcement of account access to enforce approved authorizations for:

- Logical access to VDA information and VDA resources in accordance with applicable access control policies; and
- Controlling the flow of information within the VDA and between interconnected systems and VDAs.

F-5 REMOTE ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-17)

[Licensee/Applicant]:

- Establishes and documents usage restrictions, configurations, connection requirements, and implementation guidance for each type of remote access allowed; and
- Authorizes remote access to the VDA prior to allowing such connections.

F-6 MANAGED ACCESS CONTROL POINTS
(Informed by NIST SP 800-53 Rev. 4, AC-17 (3))

[Licensee/Applicant] ensures all remote accesses to VDAs is through a boundary control device meeting the requirements in cyber security control "BOUNDARY CONTROL," of this Appendix.

F-7 WIRELESS ACCESS
(Informed by NIST SP 800-53 Rev. 4, AC-18)

[Licensee/Applicant]:

- Establishes usage restrictions, configurations, connection requirements, and implementation guidance for wireless access; and
- Authorizes wireless access to the VDA prior to allowing such connections.

F-8 RESTRICT CONFIGURATIONS BY USERS
(Informed by NIST SP 800-53 Rev. 4, AC-18 (4))

[Licensee/Applicant] identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

F-9 ANTENNAS AND TRANSMISSION POWER LEVELS
(Informed by NIST SP 800-53 Rev. 4, AC-18 (5))

[Licensee/Applicant] selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be accessed outside of licensee-controlled boundaries.

F-10 EXTERNAL INFORMATION SHARING
(Informed by NIST SP 800-53 Rev. 4, AC-21)

When VDA information is shared with external parties, [licensee/applicant]:

- Ensures that access authorizations assigned to the sharing partner match the access restrictions on the information; and
- Employs automated mechanisms to enforce these restrictions.

F-11 USE OF EXTERNAL INFORMATION SYSTEMS
(Informed by NIST SP 800-53 Rev. 4, AC-20, AC-20 (1), and AC-20 (2))

[Licensee/Applicant] establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

- Access the VDA from external information systems; and
- Process, store, or transmit organization-controlled information using external information systems.

[Licensee/Applicant]:

- Restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems; and
- Permits authorized individuals to use an external information system to access the VDA or to process, store, or transmit organization-controlled information only when the [licensee/applicant]:
  - Verifies the implementation of security controls on the external system equivalent to security controls addressed for the VDA; or
  - Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

F-12 AUDIT DATA DEFINITION, GENERATION, AND CONTENT
(Informed by NIST SP 800-53 Rev. 4, AU-3, AU-3 (1), AU-3 (2), AU-5, AU-5 (2), AU-12, AU-12 (3), AU-14, AU-14 (1), and AU-14 (2))

[Licensee/Applicant] ensures the VDA:

- Generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event; and
- Generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum:
  - Account (user or service) login failure;
  - Account role or privilege change;
  - File or object creation, modification and deletion;
  - Service start and stop;
  - Privileged service call;
  - Account creation and modification;

- Account right assignment;
- Audit policy change;
- User account password change;
- User group creation and modification; and
- Remote session start and failure.

[Licensee/Applicant] ensures the VDA auditing function:

- Alerts cyber security personnel in near real-time of an audit processing failure, or where audit failure events occur that could indicate VDA compromise;
- Takes automated measures to preserve audit data;
- Provides the capability to increase or modify audit record content in response to threat intelligence;
- Initiates session audits at VDA start-up;
- provides the capability for authorized users to select a user session to capture/record or view/hear;
- Provides the capability for authorized users to capture/record and log content related to a user session; and
- Provides centralized management and configuration of the content to be captured in audit records.

F-13 AUDIT DATA MANAGEMENT AND PROTECTION
(Informed by NIST SP 800-53 Rev. 4, AU-4, AU-5 (1), AU-9 (2), AU-9 (3), AU-9 (4), and AU-10)

[Licensee/Applicant]:

- Allocates sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configures auditing to prevent capacity from being exceeded; and
- Authorizes access to management of audit functionality to only authorized users with cyber security responsibilities.

[Licensee/Applicant] ensures the VDA:

- Provides an alert to authorized personnel when allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity;
- Backs up audit records onto a physically different system than the VDA or component being audited;
- Protects audit information and audit tools from unauthorized access, modification, and deletion;
- Implements cryptographic mechanisms to protect the integrity of audit information and audit tools; and
- Protects against an individual (or process acting on behalf of an individual) falsely denying having performed any action on the VDA.

F-14 AUDIT REVIEW, ANALYSIS, AND REPORTING
(Informed by NIST SP 800-53 Rev. 4, AU-6, AU-6a, AU-6b, AU-6 (1), and AU-6 (3))

[Licensee/Applicant]:

- Employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities;
- Reviews and analyzes VDA audit records in a timely manner for indications of potential compromise;
- Analyzes and correlates audit records across different repositories to gain organization-wide situational awareness; and

- Reports findings to the Cyber Security Team (CST).

F-15 INDEPENDENCE OF ASSESSORS
(Informed by NIST SP 800-53 Rev. 4, CA-2 (1), CA-7 (1), CA-8, and CA-8 (1))

[Licensee/Applicant]:

- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to conduct assessments of the cyber security controls;
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to monitor the cyber security controls for the VDA on an ongoing basis;
- Conducts penetration testing at least every 12 months on the VDA; and
- Utilizes assessors or assessment teams that are independent of those personnel responsible for program management or cyber security control implementation to perform penetration testing on the VDA.

F-16 SECURITY CONTROL ASSESSMENTS
(Informed by NIST SP 800-53 Rev. 4, CA-2 (2))

[Licensee/Applicant] includes and documents as part of VDA security control assessments:

- An attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
- Announced assessments:
  - In-depth monitoring (to be done automatically, in real time);
  - Vulnerability scanning (to be done at least every 30 days);
  - Malicious actor testing (to be done at least every 92 days); and
- Unannounced assessments (in addition to announced assessments above):
  - Vulnerability scanning (to be done at least every 183 days); and
  - Malicious actor testing (to be done at least every 12 months).

F-17 ENHANCEMENTS TO VDA CONNECTIONS
(Informed by NIST SP 800-53 Rev. 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant]:

- Employs a "deny-all, permit-by-exception" policy for allowing VDAs to connect to external information systems;
- Prohibits the direct connection of a VDA to an external network without the use of:
  - At least one separate, intervening access control device (e.g. firewall, cross domain solution);
  - At least one separate, intervening intrusion detection/prevention mechanism with near real-time prevention, detection and alerting capability;
  - Host-based protective measures;
  - Other measures necessary to prevent a consequence of concern; and
- Prohibits the direct connection of a VDA to a public network;
- Authorizes connections to the VDA; and
- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

F-18 CONFIGURE VDAS FOR HIGH-RISK AREAS
(Informed by NIST SP 800-53 Rev. 4, CM-2 (7))

[Licensee/Applicant] ensures the CST:

- Issues permission for individuals traveling with a VDA to locations that the [Licensee/Applicant] deems to be of significant risk; and
- Reviews the VDA upon return to ensure the device is uncompromised.

F-19 CONFIGURATION CHANGE CONTROL
(Informed by NIST SP 800-53 Rev. 4, CM-3)

[Licensee/Applicant]:

- Documents changes to the VDA that will be configuration-controlled per Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53;
- Reviews proposed configuration-controlled changes to the VDA and approves or disapproves such changes with explicit consideration for security impact analyses before implementation of the change;
- Documents configuration change decisions associated with the VDA;
- Implements approved configuration-controlled changes to the VDA;
- Retains records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements;
- Audits and reviews activities associated with configuration-controlled changes to the VDA; and
- Coordinates and provides oversight for configuration change control activities through the change management process.

F-20 CHANGE TESTING AND ANALYSIS
(Informed by NIST SP 800-53 Rev. 4, CM-3 (2) and CM-4)

[Licensee/Applicant]

- Tests, validates, and documents changes to the VDA before implementing the changes to the VDA; and
- Analyzes changes to the VDA to determine potential security impacts prior to change implementation.

F-21 ACCESS RESTRICTIONS FOR CHANGE
(Informed by NIST SP 800-53 Rev. 4, CM-5)

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

F-22 CONFIGURATION SETTINGS
(Informed by NIST SP 800-53 Rev. 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant]:

- Establishes and documents configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves any deviations from established configuration settings;
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;

- Employs automated mechanisms to centrally manage, apply, and verify VDA configuration settings; and
- Reports unauthorized changes to VDA configuration settings to the cyber security incident response team upon detection.

F-23 LEAST FUNCTIONALITY
(Informed by NIST SP 800-53 Rev. 4, CM-7)

[Licensee/Applicant]:
- Configures the VDA to provide only essential capabilities, to perform its function and maintain safe and secure operations; and
- Prohibits or restricts the use of unneeded functions, ports, protocols, and/or services.

F-24 PERIODIC REVIEW
(Informed by NIST SP 800-53 Rev. 4, CM-7 (1))

[Licensee/Applicant]:
- Reviews the VDA at least every 30 days to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
- Disables or restricts unneeded functions, ports, protocols, and/or services identified by the review.

F-25 AUTHORIZED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-7 (2) and CM-7 (4))

[Licensee/Applicant]:
- Identifies software programs authorized to execute on the VDA;
- Employs an "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA;
- Reviews and updates the list of authorized software programs, at least every 183 days; and
- Employs automated mechanisms for the VDA (i.e. application white-listing) to prevent unauthorized program execution.

F-26 VDA COMPONENT INVENTORY
(Informed by NIST SP 800-53 Rev. 4, CM-8, CM-8 (1), and CM-8 (3))

[Licensee/Applicant]:
- Develops and documents an inventory of VDA components that:
  - Accurately reflects the current VDA;
  - Includes all components within the boundary of the VDA;
  - Is at the level of granularity necessary for tracking and reporting;
  - Includes information necessary to achieve effective VDA component accountability; and
- Reviews and updates the VDA component inventory at least every 92 days or as part of any changes to a VDA;
- Updates the inventory of VDA components as an integral part of component installations, removals, and VDA updates;
- Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA; and
- Takes appropriate actions when unauthorized components are detected to remove, disable, or otherwise prevent the unauthorized component from causing a consequence of concern.

F-27 INSTALLED SOFTWARE
(Informed by NIST SP 800-53 Rev. 4, CM-11)

[Licensee/Applicant]:

- Establishes policies governing the installation of software on VDAs consistent with configuration management in 10 CFR 73.53(f);
- Enforces software installation policies using automated measures where supported; and
- Monitors policy compliance using automated measures where supported.

F-28 IDENTIFICATION AND AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-2, IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (8), IA-2 (11), IA-2 (12), IA-3, and IA-8)

[Licensee/Applicant] ensures the VDA:

- Uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and non-organizational users (or processes acting on behalf of non-organizational users);
- Implements multifactor authentication for network access to privileged accounts;
- Implements multifactor authentication for network access to non-privileged accounts;
- Implements multifactor authentication for local access to privileged accounts;
- Implements replay-resistant authentication mechanisms for network access to privileged accounts;
- Implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets E-authentication Assurance Level 3 as described in NIST SP 800-63-2 or later revisions;
- Accepts and electronically verifies Personal Identity Verification credentials; and
- Uniquely identifies and authenticates devices before establishing a connection to a VDA.

F-29 IDENTIFIER MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-4)

[Licensee/Applicant] manages VDA identifiers by:

- Receiving independent management authorization to assign an individual, group, role, or device identifier;
- Selecting an identifier that identifies an individual, group, role, or device;
- Assigning the identifier to the intended individual, group, role, or device; and
- Preventing reuse of identifiers where reuse could allow unintended or unauthorized access; and
- Disabling the identifier within 60 days of inactivity.

F-30 AUTHENTICATOR MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the organization;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;

- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators prior to VDA installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- Documenting authenticator types approved for use, the frequency for changing/refreshing, and the technical justification that demonstrates that adequate security is provided by the frequency;
- Protecting authenticator content from unauthorized disclosure and modification;
- Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- Changing authenticators for group/role accounts when membership to those accounts changes.

F-31 PASSWORD-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (1))

[Licensee/Applicant] ensures that password-based authentication for the VDA:

- Enforces a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security;
- Enforces password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters;
- Enforces a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries;
- Stores and transmits only cryptographically-protected passwords;
- Enforces lifetime restrictions for password minimums of 1 day and provides a technical basis for maximums defined and documented by the CST that prevents unauthorized access;
- Prohibits password reuse for 10 generations; and
- When temporary passwords are used for VDA logons, an immediate change to a permanent password is required upon the first logon.

[Licensee/Applicant] ensures that written or electronic copies of master passwords are stored in a secure location with limited access.

F-32 PUBLIC KEY INFRASTRUCTURE (PKI)-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (2))

[Licensee/Applicant] ensures that PKI-based authentication for the VDA:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
- Enforces authorized access to the corresponding private key;
- Maps the authenticated identity to the account of the individual or group; and
- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

F-33 HARDWARE TOKEN-BASED AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-5 (11))

[Licensee/Applicant] ensures that hardware token-based authentication for the VDA, employs mechanisms that satisfy E-authentication Assurance Level 3 as described in NIST SP 800-63-2 or later revisions.

F-34 AUTHENTICATOR FEEDBACK
(Informed by NIST SP 800-53 Rev. 4, IA-6)

[Licensee/Applicant] ensures the VDA obscures feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

F-35 CRYPTOGRAPHIC MODULE AUTHENTICATION
(Informed by NIST SP 800-53 Rev. 4, IA-7)

[Licensee/Applicant] ensures the VDA implements mechanisms for authentication to a cryptographic module based on NIST Cryptographic Module Validation Program (CMVP) and associated guidance for such authentication.

F-36 INCIDENT RESPONSE TRAINING
(Informed by NIST SP 800-53 Rev. 4, IR-2)

[Licensee/Applicant] provides incident response training to VDA users consistent with assigned roles and responsibilities:

- Within 92 days of assuming an incident response role or responsibility;
- When required by VDA changes; and
- At least every 12 months.

F-37 INCIDENT RESPONSE TESTING
(Informed by NIST SP 800-53 Rev. 4, IR-3 and IR-3 (2))

[Licensee/Applicant]:

- Tests the incident response capability for the VDA at least every 92 days using one or more of the following methods to determine the incident response effectiveness and documents the results of checklists, walk-through or tabletop exercises, and simulations (parallel/full interrupt).
- Tests the incident response capability for the VDA at least every 36 months using a comprehensive exercise; and
- Coordinates incident response testing with organizational elements responsible for related plans.

F-38 INCIDENT HANDLING
(Informed by NIST SP 800-53 Rev. 4, IR-4 and IR-4 (1))

[Licensee/Applicant]:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities;
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly; and
- Utilizes automated mechanisms to support the incident handling process.

F-39 INCIDENT MONITORING
(Informed by NIST SP 800-53 Rev. 4, IR-5)

[Licensee/Applicant] tracks and documents VDA security incidents.

F-40 INCIDENT REPORTING
(Informed by NIST SP 800-53 Rev. 4, IR-6 and IR-6 (1))

[Licensee/Applicant]:

- Requires personnel to report suspected cyber security incidents to the CST upon discovery; and
- Employs automated mechanisms to assist in the reporting of security incidents.

F-41 INCIDENT RESPONSE ASSISTANCE
(Informed by NIST SP 800-53 Rev. 4, IR-7 and IR-7 (1))

[Licensee/Applicant]:

- Provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the VDA for the handling and reporting of security incidents; and
- Employs automated mechanisms to increase the availability of incident response-related information and support.

F-42 CONTROLLED MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-2)

[Licensee/Applicant]:

- Performs and documents maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern;
- Reviews records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days;
- Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Requires that CST approve the removal of the VDA for off-site maintenance or repairs outside the licensees positive control;
- Sanitizes equipment to remove all information from associated media prior to removal for off-site maintenance or repairs outside the licensees positive control;
- Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions;
- Includes in records of maintenance and repairs on VDA components at a minimum: date, time, identification of those performing the maintenance, description of maintenance performed, and VDA components removed or replaced; and
- Retains records for inspection by the NRC.

F-43 MAINTENANCE TOOLS
(Informed by NIST SP 800-53 Rev. 4, MA-3, MA-3 (1), and MA-3 (2))

[Licensee/Applicant]:

- Approves, controls, and monitors VDA maintenance tools;
- Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications; and
- Checks media containing diagnostic and test programs for malicious code before the media are used in the VDA.

F-44 NONLOCAL MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant]:
- Approves and monitors nonlocal maintenance and diagnostic activities;
- Documents and only allows the use of nonlocal maintenance and diagnostic tools for the VDA where those tools do not introduce vulnerabilities or lead to a consequence of concern (e.g., information systems that perform maintenance on VDAs are protected equivalent to the VDA);
- Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
- Maintains records for nonlocal maintenance and diagnostic activities; and
- Terminates session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant]:
- Documents the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections; or
- Removes the component to be serviced from the VDA prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to VDA information) before removal from licensee facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the VDA.

F-45 MAINTENANCE PERSONNEL
(Informed by NIST SP 800-53 Rev. 4, MA-5)

[Licensee/Applicant]:
- Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- Ensures that unescorted personnel performing maintenance on the VDA have required access authorizations; and
- Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

F-46 TIMELY MAINTENANCE
(Informed by NIST SP 800-53 Rev. 4, MA-6)

[Licensee/Applicant] obtains maintenance support and/or spare parts for VDAs that must remain operational to prevent a consequence of concern.

F-47 MEDIA ACCESS
(Informed by NIST SP 800-53 Rev. 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media includes any active storage device, passive storage device or passive media that:
- Contain information used to manage, configure, maintain, secure or operate the VDA; or
- Are used on the VDA for any purpose.

F-48 MEDIA MARKING
(Informed by NIST SP 800-53 Rev. 4, MP-3)

[Licensee/Applicant] marks VDA media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

F-49 MEDIA STORAGE
(Informed by NIST SP 800-53 Rev. 4, MP-4)

[Licensee/Applicant]:

- Physically controls and securely stores VDA media; and
- Protects VDA media until the media are destroyed or sanitized using approved equipment, techniques, and procedures that would prevent recovery of the data by an adversary.

F-50 MEDIA TRANSPORT
(Informed by NIST SP 800-53 Rev. 4, MP-5 and MP-5 (4))

[Licensee/Applicant]:

- Protects and controls VDA media during transport outside of controlled areas;
- Maintains accountability for VDA media during transport outside of controlled areas;
- Documents activities associated with the transport of VDA media;
- Restricts the activities associated with the transport of VDA media to authorized personnel; and
- Implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

F-51 MEDIA SANITIZATION
(Informed by NIST SP 800-53 Rev. 4, MP-6)

[Licensee/Applicant]:

- Sanitizes VDA media prior to disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary; and
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

F-52 MEDIA USE
(Informed by NIST SP 800-53 Rev. 4, MP-7)

[Licensee/Applicant] prohibits the use of any media with a VDA, except specifically approved VDA media.

F-53 VULNERABILITY SCANNING
(Informed by NIST SP 800-53 Rev. 4, RA-5, RA-5 (1), RA-5 (2), and RA-5 (5))

[Licensee/Applicant]:

- Scans for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA, applications or both are identified and reported;
- Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting checklists and test procedures;

  - Measuring vulnerability impact; and
- Analyzes vulnerability scan reports and results from security control assessments;
- Addresses vulnerabilities in a timely and technically justified manner to prevent a consequence of concern;
- Shares information obtained from the vulnerability scanning process and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other VDAs (i.e., systemic weaknesses or deficiencies);
- Employs vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned;
- Updates the VDA vulnerabilities scanned prior to a new scan; and
- Implements privileged access authorization to the VDA for vulnerability scanning activities.

F-54 EXTERNAL INFORMATION SYSTEM SERVICES
(Informed by NIST SP 800-53 Rev. 4, SA-9 and SA-9 (2))

[Licensee/Applicant]:
- Requires that providers of external information system services that interact with VDAs comply with information security requirements and address security controls for the associated consequence of concern;
- Defines and documents oversight and user roles and responsibilities with regard to external information system services;
- Employs automated mechanisms to monitor security control compliance by external service providers on an ongoing basis; and
- Requires providers of external information system services that interact with VDAs to identify the functions, ports, protocols, and other services required for the use of such services.

F-55 DEVELOPER CONFIGURATION MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SA-10)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to:
- Perform configuration management during the VDA, component, or service lifecycle;
- Document, manage, and control the integrity of changes to the VDA, component, or service;
- Implement only organization-approved changes to the VDA, component, or service;
- Document approved changes to the VDA, component, or service and the potential security impacts of such changes; and
- Track security flaws and flaw resolution within the VDA, component, or service and report findings to CST.

F-56 DEVELOPER SECURITY TESTING AND EVALUATION
(Informed by NIST SP 800-53 Rev. 4, SA-11)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to:
- Create and implement a security assessment plan;
- Perform comprehensive cyber security testing and evaluation;
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- Implement a verifiable flaw remediation process; and

- Correct flaws identified during security testing and evaluation.

F-57 SYSTEM PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-2 and SC-4)

[Licensee/Applicant]:
- Separates user functionality of the VDA (including user interface services) from VDA management functionality; and
- Prevents unauthorized and unintended information transfer via shared resources.

F-58 DENIAL OF SERVICE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-5)

[Licensee/Applicant] protects against or limits the effects of denial of service attacks by employing technical safeguards and countermeasures.

F-59 BOUNDARY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SC-7, SC-7 (3), SC-7 (4), SC-7 (5), and SC-7 (7))

[Licensee/Applicant] ensures the VDA:
- Monitors and controls communications at the boundary of the VDA and at key internal boundaries within the VDA;
- Implements subnetworks for publicly or externally accessible VDA components that are physically or logically separated from internal [licensee/applicant] networks;
- Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security architecture; and
- Denies network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

[Licensee/Applicant] limits the number of external network connections to the VDA.

F-60 EXTERNAL TELECOMMUNICATIONS SERVICES
(Informed by NIST SP 800-53 Rev. 4, SC-7 (4), SC-7 (5), SC-7 (7), SC-7 (8), SC-7 (10), SC-7 (11), SC-7 (12), SC-7 (14), SC-7 (18), SC-7 (20), and SC-7 (21))

[Licensee/Applicant]:
- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- Reviews exceptions to the traffic flow policy on a timely basis and removes exceptions that are no longer supported by an explicit mission/business need;
- Implements a managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;

- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
- Reviews exceptions to the traffic flow policy at least every 30 days and removes exceptions that are no longer supported by an explicit mission/business need;
- Prevents the unauthorized exfiltration of information across managed interfaces;
- Allows only incoming communications from authorized sources to be routed to VDAs;
- Implements host-based firewalls on VDAs;
- Protects against unauthorized physical connections to the VDA; and
- Employs boundary protection mechanisms.

[Licensee/Applicant] ensures the VDA:

- Has managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception);
- Prevents, in conjunction with a remote device, the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks;
- Routes internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
- Provides the capability to dynamically isolate/segregate VDAs from other VDAs; and
- Fails securely and safely in the event of an operational failure of a boundary protection device.

F-61 TRANSMISSION CONFIDENTIALITY AND INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures the VDA:

- Protects the confidentiality and integrity of transmitted information; and
- Implements cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to information during transmission, unless the transmission medium is otherwise protected by alternative physical safeguards.

F-62 NETWORK DISCONNECT
(Informed by NIST SP 800-53 Rev. 4, SC-10)

[Licensee/Applicant] terminates the network connection associated with a VDA communications session at the end of the session or within 10 minutes of inactivity, except for communications sessions that are necessary for safe operation of the VDA or are necessary to prevent a consequence of concern,

F-63 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
(Informed by NIST SP 800-53 Rev. 4, SC-12 and SC-12 (1))

[Licensee/Applicant]:

- Establishes and manages cryptographic keys for required cryptography employed within the VDA in accordance with NIST CMVP; and
- Maintains availability of information necessary to safely operate the VDA or prevent a consequence of concern in the event of the loss of cryptographic keys by users.

F-64 COLLABORATIVE COMPUTING DEVICES
(Informed by NIST SP 800-53 Rev. 4, SC-15)

[Licensee/Applicant] ensures the VDA:

- Prohibits remote activation of collaborative computing devices except where explicitly authorized; and
- Provides an explicit indication of use to users physically present at the devices.

F-65 PUBLIC KEY INFRASTRUCTURE CERTIFICATES
(Informed by NIST SP 800-53 Rev. 4, SC-17)

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

F-66 VOICE OVER INTERNET PROTOCOL (VOIP)
(Informed by NIST SP 800-53 Rev. 4, SC-19)

[Licensee/Applicant]:

- Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the VDA if used maliciously; and
- Authorizes, monitors, and controls the use of VoIP within the VDA.

F-67 SECURE NAME / ADDRESS RESOLUTION
(Informed by NIST SP 800-53 Rev. 4, SC-20, SC-20a, SC-21, and SC-22)

[Licensee/Applicant] ensures the VDA:

- Provides additional data origin authentication and integrity verification artifacts for the VDA along with the authoritative name resolution data the VDA returns in response to external name/address resolution queries;
- Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace;
- Requests and performs data origin authentication and data integrity verification on the name/address resolution responses the VDA receives from authoritative sources; and
- Collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

F-68 SESSION AUTHENTICITY
(Informed by NIST SP 800-53 Rev. 4, SC-23)

[Licensee/Applicant] ensures the VDA protects the authenticity of communications sessions.

F-69 PROTECTION OF INFORMATION AT REST
(Informed by NIST SP 800-53 Rev. 4, SC-28)

[Licensee/Applicant] protects the confidentiality and integrity of VDA information at rest.

F-70 PROCESS ISOLATION
(Informed by NIST SP 800-53 Rev. 4, SC-39)

[Licensee/Applicant] maintains a separate execution domain for each executing process.

F-71 FLAW REMEDIATION
(Informed by NIST SP 800-53 Rev. 4, SI-2 and SI-2 (2))

[Licensee/Applicant]:

- Identifies, reports, and corrects VDA flaws;
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- Correcting the flaw expeditiously using the configuration management process;
- Incorporates flaw remediation into the organizational configuration management process;
- Performs vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production; and
- Employs automated mechanisms to determine the state of VDA components with regard to flaw remediation.

F-72 MALICIOUS CODE PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-3, SI-3 (1), and SI-3 (2))

[Licensee/Applicant]:

- Employs malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code;
- Updates malicious code protection mechanisms whenever new releases are available;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the VDA at least every 7 days;
  - Perform real-time scans of files from external sources as the files are downloaded, opened, or executed;
  - Prevent malicious code execution;
  - Alert the CST of the detection of malicious code in a timely manner; and
- Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA;
- Centrally manages malicious code protection mechanisms; and
- Automatically updates malicious code protection mechanisms for the VDA.

F-73 VDA MONITORING
(Informed by NIST SP 800-53 Rev. 4, SI-4, SI-4 (2), SI-4 (4), and SI-4 (5))

[Licensee/Applicant]:

- Monitors the VDA to detect:
  - Cyber attacks and indicators of potential cyber attacks;
  - Unauthorized local, network, and remote connections; and
- Identifies unauthorized use of the VDA using automated or other means;
- Deploys monitoring devices:
  - Strategically within the VDA to collect organization-determined essential information;
  - At ad hoc locations within the system to track specific types of transactions of interest to the organization; and

- Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- Heightens the level of VDA 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;
- Provides VDA monitoring information to appropriate licensee cyber security personnel as necessary;
- Employs automated tools to support near real-time analysis of events;
- Monitors inbound and outbound communications traffic for the VDA in near real-time for unusual or unauthorized activities or conditions; and
- Ensures appropriate cyber security personnel are alerted when indications of compromise or potential compromise of the VDA occurs.

F-74 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
(Informed by NIST SP 800-53 Rev. 4, SI-5)

[Licensee/Applicant]:

- Receives cyber security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis;
- Generates internal security alerts, advisories, and directives as necessary;
- Disseminates security alerts, advisories, and directives to appropriate personnel and the NRC; and
- Implements security directives in a timely manner.

F-75 SECURITY FUNCTION VERIFICATION
(Informed by NIST SP 800-53 Rev. 4, SI-6 and SI-6 (3))

[Licensee/Applicant]:

- Verifies the correct operation of security functions;
- Performs this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and when anomalies are discovered;
- Notifies appropriate personnel in a timely manner of failed security verification tests; and
- Reports the results of security function verification to the CST.

F-76 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
(Informed by NIST SP 800-53 Rev. 4, SI-7, SI-7 (1), SI-7 (2), SI-7 (5), SI-7 (7), SI-7 (12), SI-7 (12), SI-7 (14))

[Licensee/Applicant]:

- Employs integrity verification tools to detect unauthorized changes to VDA software, firmware, and information;
- Performs an integrity check of VDA software, firmware, and information that occurs, where possible, upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and when anomalies are discovered; and
- Incorporates the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability.

F-77 ERROR HANDLING
(Informed by NIST SP 800-53 Rev. 4, SI-11)

[Licensee/Applicant] ensures the VDA:

- Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- Reveals error messages only to personnel responsible for VDA operation and maintenance.

F-78 INFORMATION HANDLING AND RETENTION
(Informed by NIST SP 800-53 Rev. 4, SI-12)

[Licensee/Applicant] handles and retains information within the VDA and information output from the VDA in accordance with NRC record retention requirements.

F-79 MEMORY PROTECTION
(Informed by NIST SP 800-53 Rev. 4, SI-16)

[Licensee/Applicant] implements automated mechanisms and safeguards for the VDA to protect its memory from unauthorized code execution.

APPENDIX G

EXAMPLE IMPLEMENTING PROCEDURE

This is an example implementing procedure for a single access control VDA.

- Reference a network diagram and provide a physical location for the VDA.
- Identification of the VDA and boundary would include:
    - Computer system (name and model);
    - Computer monitor (name and model);
    - Printer (name and model);
    - Access control and alarm cabinet (name and model);
    - Card readers (name and model); and
    - Door alarm contacts (name and model).
- Type of consequence of concern:
    - Latent – safeguards
- Function, general description, and purpose of the VDA - The description of an access control and alarm system is as follows:

> "The access control and alarm system performs a security function and is responsible for maintaining and monitoring access control to a controlled access area (CAA) storing special nuclear material. In addition, the system monitors door alarm contacts leading into and exiting the CAA. The alarm contacts generate intrusion, tamper, or trouble alarms that are displayed and annunciated on the computer system in the event of an alarm condition. The computer system is located in a manned security station and is kept under observation. The access control and alarm cabinet is locked and alarmed (tamper) and is located within the manned station with the computer system. The data lines to and from the card readers and the alarm contacts to the access control and alarm cabinet are supervised. In the event of a device or system failure compensatory measures are implemented in accordance with site procedures [reference the procedure]."

- Individual(s) or organization responsible for the VDA - For the access control and alarm system, the following parties are responsible for the various major components:
    - Access Control and Alarm System (Security Department);
    - Computer system (Information Technology (IT) Department);
    - Computer monitor (IT Department);

- Printer (IT Department);
- Access control and alarm cabinet (Security Department);
- Card readers (Security Department); and
- Door alarm contacts (Security Department).

- Location, interconnections, and environment;

  This VDA is located in security station #5 on the second floor. It is connected into the security system network using jack T-5 by means of a Category 5 data cable. It is housed in temperature controlled equipment cabinet 5-11.

- Support systems for the VDA;

  "The access control and alarm system relies on a number of support systems including:

  - Electrical power supply (not a VDA because the system fails safe); and
  - Communications between the detectors and alarm system (VDA, see procedure [LICENSEE SPECIFIED PROCEDURE NUMBER])."

- Support systems for the VDA;

  "The access control and alarm system uses the following tools for calibration and configuration:

  - Hex wrench size X to open the faceplate (not a VDA)
  - Configuration laptop computer (VDA, see procedure [LICENSEE SPECIFIED PROCEDURE NUMBER])."

- Inventory (hardware, software, versions);

  Inventory for the access control and alarm system VDA may include the following:

  - Computer system – [LICENSEE SPECIFIED LIST OF SOFTWARE AND PROGRAMS INSTALLED (E.G., OPERATING SYSTEM, ACCESS CONTROL AND ALARM SOFTWARE) ALONG WITH LATEST VERSIONS, UPDATES AND PATCHES].
  - [LICENSEE SPECIFIED LIST OF PERIPHERALS ATTACHED TO OR USED WITH THE COMPUTER SYSTEM AS WELL.]
  - Access control and alarm cabinet – [LICENSEE SPECIFIED LIST OF THE TYPES OF CARDS, CONTROLLERS OR MODULES INSTALLED ALONG WITH THE LATEST SOFTWARE AND FIRMWARE INSTALLED.]

- Standards and applicable cyber security controls.

  - Specific cyber security control X-XX for local access control accounts was not applied because the VDA is in a locked and alarmed room and no attack path exists.

- Specific cyber security control Y-YY involving protected data communications was applied but it is inherited from the security system network (also a VDA) and the firewall installed there as a measure to meet that control's standard.

- Specific cyber security control Z-ZZ involving data at rest was applied. The VDA was configured such that all ports except the network connection are disabled. This measure is tested by plugging in an approved USB device to confirm the settings. The test results are to be sent to the cyber security team and housed in the maintenance documents for this VDA.