U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

January 2017
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 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) 73.53, "Requirements for cyber security at nuclear fuel cycle facilities" (Ref. 1).

Applicability

This RG applies to each FCF applicant or licensee subject to the requirements of 10 CFR 73.53 (hereinafter, these applicants and licensees will be referred to collectively as "a licensee" or "the licensee").

Applicable Regulations

- 10 CFR Part 40, "Domestic Licensing of Source Material," (Ref. 2) establishes the requirements for domestic licensing of source material.
- 10 CFR 40.31, "License applications," (Ref. 3) establishes the interface and requirements for cyber security plans, as required by 10 CFR 73.53, for a licensee possessing source material at a FCF for the production, conversion, or deconversion of uranium hexafluoride.
- 10 CFR 40.35(g), "Conditions of specific licenses issued pursuant to 10 CFR 40.34," (Ref. 4) establishes the interface and requirements for the process to change cyber security plans, as

required by 10 CFR 73.53, for a licensee possessing source material at a FCF for the production, conversion, or deconversion of uranium hexafluoride.

- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," (Ref. 5) establishes the requirements for domestic licensing of special nuclear material (SNM).

- 10 CFR 70.22, "Contents of application," (Ref. 6) establishes the interface and requirements for cyber security plans, as required by 10 CFR 73.53, for a licensee possessing greater than a critical mass of SNM and engaging in specific fuel cycle activities.

- 10 CFR 70.32(f), "Conditions of licenses," (Ref. 7) establishes the interface and requirements for the process to change cyber security plans, as required by 10 CFR 73.53, for a licensee possessing greater than a critical mass of SNM and engaging in specific fuel cycle activities.

- 10 CFR Part 70.61, "Performance requirements," (Ref. 8) establishes the performance requirements for an integrated safety analysis.

- 10 CFR Part 70.62, "Safety program and integrated safety analysis," (Ref. 9) establishes the requirements for establishing a safety program and performing an integrated safety analysis.

- 10 CFR Part 73, "Physical Protection of Plants and Materials," (Ref. 10) establishes requirements for the physical protection of SNM.

- 10 CFR Part 73.1(a)(1), "Radiological sabotage," (Ref. 11) establishes the design basis threat (DBT) for radiological sabotage.

- 10 CFR Part 73.1(a)(2), "Theft or diversion of formula quantities of strategic special nuclear material," (Ref. 12) establishes the DBT for theft or diversion of formula quantities of strategic SNM.

- 10 CFR Part 73.20, "General performance objective and requirements," (Ref. 13) establishes requirements of a physical protection system for formula quantities of strategic SNM.

- 10 CFR Part 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance," (Ref. 14) establishes requirements for the physical protection of SNM of moderate and low strategic significance.

- 10 CFR 73.46(g)(6), "Fixed site physical protection systems, subsystems, components, and procedures," (Ref. 15) establishes the process and requirements for the annual review of security and cyber security programs for a licensee possessing a formula quantity of strategic SNM.

- 10 CFR 73.53, "Requirements for cyber security at nuclear fuel cycle facilities," establishes requirements for an FCF licensee to establish, implement, and maintain a cyber security program that detect, protect against, and respond to a cyber attack capable of causing a consequence of concern.

- 10 CFR 73.54, "Protection of digital computer and communication systems and networks," (Ref. 16) establishes the requirements for cyber security at operating power reactors and combined license applicants.

- 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material," (Ref. 17) establishes requirements for the control and accounting of SNM applicable to a licensee and for documenting the transfer of SNM.

- 10 CFR Part 74.41, "Nuclear material control and accounting for special nuclear material of moderate strategic significance," (Ref. 18) establishes requirements for the control and accounting of SNM of moderate strategic significance.

- 10 CFR Part 74.51, "Nuclear material control and accounting for strategic special nuclear material," (Ref. 19) establishes requirements for the control and accounting of formula quantities of strategic SNM.

- 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," (Ref. 20) establishes the procedures for obtaining a facility security clearance and for safeguarding Secret and Confidential National Security Information and Restricted Data.

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," (Ref. 21) describes the adversary characteristics, tactics, techniques, and procedures to assist a licensee possessing a formula quantity of strategic SNM (i.e., Category I FCF licensees) to further develop their protective strategies against the DBT and provides guidance on how site-specific security plans should consider the DBT.

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 events, and to provide guidance to applicants. Regulatory guides 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. This RG applies to FCF subject to the requirements in 10 CFR 73.53.

Paperwork Reduction Act

This regulatory guide contains new or amended collections of information subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). The collections of information were approved by the Office of Management and Budget, approval 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 collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

TABLE OF CONTENTS

B. DISCUSSION

Reason for Issuance

This RG provides a FCF licensee with an acceptable approach for meeting the requirements of 10 CFR 73.53. It also provides a methodology that the licensee may use to establish, implement, and maintain a cyber security program that detects, protects against, and responds 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 associated with a consequence of concern and a process to determine which of those digital assets require protection from cyber attacks. This RG also 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 through 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, (3) the potential for these attacks to impact numerous digital assets, including digital assets used at nuclear FCFs, and (4) the emergence of these attacks to produce kinetic effects. 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 the occurrence of certain potential consequences caused by a physical attack on a FCF licensee. These orders addressed the threat environment at that time by imposing additional security requirements beyond those in 10 CFR Part 73. 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 NRC issued: "Issuance of Order for Interim Compensatory Measures – Global Nuclear Fuel – Americas, LLC Wilmington, NC," on February 06, 2003 (Ref. 22); "Issuance of Order for Interim Compensatory Measures – Framatome Advanced Nuclear Power, Inc. Richland, WA," on February 06, 2003 (Ref. 23); "Issuance of Order for Interim Compensatory Measures – Westinghouse Electric Company LLC Columbia, SC," on February 06, 2003 (Ref. 24); "Issuance of Order for Interim Compensatory Measures – Nuclear Fuel Services, Inc. Irwin, TN," on February 06, 2003 (Ref. 25); "Issuance of Order for Interim Compensatory Measures – BWX Technologies Lynchburg, VA," on April 29, 2003 (Ref. 26); and "Issuance of Order for Interim Compensatory Measures – Honeywell International, Inc. Metropolis, IL" on August 18, 2004 (Ref. 27). These interim compensatory measures orders contained a generic cyber security measure directing licensees to evaluate and address cyber security vulnerabilities. FCFs licensed after 2003 had the requirements of the orders either incorporated as license conditions or issued as separate orders. This generic cyber security requirement did not specify or provide guidance for a FCF licensee 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 issued a rulemaking entitled, "Design Basis Threat" (Volume 72 of the *Federal Register*, page 12705 (72 FR 12705; March 19, 2007)) (Ref. 28), revising portions of 10 CFR Part 73 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. The NRC developed RG 5.70 to further

describe the adversary characteristics, tactics, techniques, and procedures to assist a Category I FCF licensee to further develop their protective strategies against the DBT. RG 5.70 provides guidance on how site-specific security plans should consider the DBT, but it does not provide a FCF licensee with guidance on detecting, protecting against, or responding to a cyber attack.

In March 2009, the NRC further addressed cyber security through the publication of the "Power Reactor Security Requirements" final rule *Federal Register* notice (74 FR 13926; March 27, 2009) (Ref. 29). The cyber security requirements for power reactors were placed into 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." The cyber security rule requires that 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. 30).

In June 2012, the NRC staff completed SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," dated June 25, 2012 (Ref. 31), which established the NRC staff's approach for evaluating the need for cyber security requirements for four categories of NRC licensees and facilities: (1) FCFs, (2) nonpower 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," dated December 30, 2014 (Ref. 32). 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, "Staff Requirements – SECY-14-0147 – Cyber Security for Fuel Cycle Facilities," (Ref. 33), 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 applicable type of consequence of concern and a process for determining which digital assets should be protected from cyber attacks. Digital assets that should be protected are referred to as "vital digital assets" (VDAs). In accordance with 10 CFR 73.53(d)(5), a licensee protects 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. A licensee may use the cyber security controls provided in the appendices to this RG or develop their own sets of cyber security controls and submit them within their cyber security plan for NRC review and approval. Licensees developing cyber security controls to satisfy the stated regulatory requirements should base the controls on industry accepted standards (e.g., National Institute of Standards and Technology (NIST) or the joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC)).

This RG provides guidance on the requirements of 10 CFR 73.53. In addition, this guidance provides a licensee an acceptable methodology to address 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.

Section C, "Staff Regulatory Guidance," of this RG provides an overview of the specific requirements and the expectations for this method of meeting the requirements of 10 CFR 73.53. Appendix A contains a template that provides an example of an acceptable format and content for the cyber security plan that the licensee submits to the NRC in accordance with 10 CFR 73.53(a). A licensee may use the template to assist in documenting compliance with the regulatory requirements, and the NRC can use it to assist in the review process. Appendices B, C, D, E, and F contain cyber security controls that are specific to each type of consequence of concern and acceptable to the NRC staff for establishing the performance specifications of the measures taken to protect VDAs. Appendix G contains an example of an implementing procedure to assist the licensee in developing site-specific implementing procedures for VDAs.

The cyber security controls in Appendices B through F of this RG are informed by the NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, issued April 2013 (Ref. 34), and NIST SP 800 82, "Guide to Industrial Control Systems (ICS) Security," Revision 2, issued May 2015 (Ref. 35). In addition, the NRC took lessons learned from its own cyber security guidance for nuclear power reactors (RG 5.71). Further, the NRC has modeled its expectations for a FCF licensee after the NIST "Framework for Improving Critical Infrastructure Cyber Security," Version 1, issued February 2014 (Ref. 36), and its "Manufacturing Profile," issued April 2016 (draft) (Ref. 37). 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, however the use of these references by this document does not constitute endorsement of these references.

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 December 2011 (Ref. 38), 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. 39), addresses steps required to effectively execute an information security plan and discusses cyber security issues. More specifically, 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. 40), discusses the challenges of addressing cyber security in the context of implementing and maintaining digital instrumentation and control systems. Although these documents discuss cyber security, their intended use is for a nuclear power reactor rather than a FCF licensee. For this reason, this RG incorporates similar concepts and is consistent with the basic cyber security principles provided in IAEA Nuclear Security Series Nos. 17 and 23-G and IAEA Nuclear Energy Series Technical Report NP-T-1.13.

The NRC staff also reviewed the ISO/IEC 27000 series entitled, "Information Security Management System (ISMS), Family of Standards" (Ref. 41). This family of standards, revised in 2016, provides 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 2012 (Ref. 42), 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 are 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.

C. STAFF REGULATORY GUIDANCE

1 General Requirements

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 cyber security controls specific to consequences of concern.

The provisions of 10 CFR 73.53 identify the requirements needed to meet the cyber security program performance objectives for a FCF licensee. The cyber security program performance objectives identified in 10 CFR 73.53(b) provide the requirement for a licensee to establish, implement, and maintain a cyber security program that detects, protects against, and responds to a cyber attack capable of causing a consequence of concern. The rule identifies four types of consequences of concern (see Table C-1) that establish thresholds for potential events involving radiological and chemical exposures, classified information or matter, SNM of moderate strategic significance, and a formula quantity of strategic SNM. Preventing these events protects public health and safety and promotes the common defense and security. The cyber security program includes (1) establishing and maintaining a Cyber Security Team (CST), (2) developing a site-specific cyber security plan that the licensee submits 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 whether 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 cyber security temporary compensatory measures (TCMs) to meet the 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), the licensee establishes and maintains an adequately structured CST consisting of appropriately 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 is responsible for implementing a cyber security program that meets the requirements of 10 CFR 73.53. Section C.3 provides additional guidance on the CST. An effective team has the appropriate resources available to execute their CST responsibilities.

1.2 Cyber Security Plan

In accordance with 10 CFR 73.53(e), a licensee establishes, implements, and maintains a site-specific cyber security plan. The provisions of 10 CFR 73.53(a) provide the requirements for a current licensee to submit, through an application for amendment of their license, a cyber security plan for NRC review and approval. The provisions of 10 CFR 40.31 or 10 CFR 70.22, as appropriate, provide the requirements for a future licensee (i.e., applicant) 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 its compliance with 10 CFR 73.53. To meet the requirements of 10 CFR 73.53(e)(1), the cyber security plan: (1) documents that the CST is adequately structured, staffed, trained, qualified, and equipped to manage the cyber security program; and (2) specifies the cyber security controls that the licensee addresses to protect VDAs from cyber attacks and prevent consequences of concern. In accordance with 10 CFR 73.53(e)(2), the cyber security plan

describes the licensee's measures for (1) management and performance of the cyber security program and (2) incident response to a cyber attack affecting VDAs. Upon implementation of the licensee's approved cyber security plan, the NRC will periodically inspect the cyber security program for its compliance with 10 CFR 73.53. Section C.4 provides additional guidance on the cyber security plan. Appendix A contains a template that provides an example of an acceptable format and content for the cyber security plan that the licensee submits 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), a licensee identifies digital assets associated with a type of consequence of concern and further evaluates whether an alternate means (protected from a cyber attack) is available that prevents the consequence of concern in the event that a cyber attack compromises the digital asset. Section C.6 provides additional guidance on the identification of digital assets.

In accordance with 10 CFR 73.53(d)(4), a licensee determines 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 if the alternate means cannot be compromised by a cyber attack. The regulation in 10 CFR 73.53(d)(5) requires only VDAs to be protected against a cyber attack. As part of this analysis, the licensee also identifies 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. Section C.6 provides additional guidance on the identification of VDAs.

1.4 Addressing Performance Specifications of Cyber Security Controls

In accordance with 10 CFR 73.53(d)(2) and (d)(5), a licensee takes measures for each VDA to address the performance specifications of the applicable cyber security controls based on the type of consequence of concern. The licensee may elect to group similar types of VDAs together to allow them 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 is prevented. Section C.7 provides additional guidance on cyber security controls. Appendices B, C, D, E, and F 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 sets of controls for NRC review and approval in the cyber security plan.

1.5 Implementing Procedures and Temporary Compensatory Measures

In accordance with 10 CFR 73.53(5)(ii), the licensee establishes and maintains written implementing procedures for VDAs and documents 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. Section C.8 provides additional guidance on implementing procedures.

In accordance with 10 CFR 73.53(d)(6), the licensee applies TCMs when the measures taken to address the performance specifications associated with the identified cyber security controls are degraded. When implemented, TCMs are documented and tracked to completion. Documentation associated with the TCM is made available for inspection by the NRC staff. These TCMs may be identified in the

implementing procedures, or they could be part of other site-specific documentation. Section C.8 provides additional guidance on TCMs.

1.6 Managing the Cyber Security Program

As required by 10 CFR 73.53(e)(1), a cyber security plan describes how the licensee satisfies the regulatory requirements and manages 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. For this reason, the licensee management of the cyber security program is needed to maintain its effectiveness and adequacy. The provisions of 10 CFR 73.53(f) through (i) provide requirements for configuration management, review of the cyber security program, event reporting and tracking, and recordkeeping. The provisions of 10 CFR 73.53(f) through (i) establish the requirements for management of the cyber security program over the life of the facility. These elements of the cyber security program should be incorporated in, and conducted as part of, the licensee's standard operations. This RG contains additional guidance in Section C.9, for configuration management; Section C.10, for review of the cyber security program; Section C.11, for event reporting and tracking; and Section C.12, for recordkeeping.

2 Cyber Security Program Performance Objectives

In accordance with 10 CFR 73.53(b), a licensee establishes, implements, and maintains a cyber security program that detects, protects against, and responds to a cyber attack capable of causing a consequence of concern. The cyber security requirements established in 10 CFR 73.53 are intended to be risk-informed and performance based to allow the licensee 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.

2.1 Detect a Cyber Attack Capable of Causing a Consequence of Concern

As required by 10 CFR 73.53(b), the licensee implements a cyber security program that detects a cyber attack capable of causing a consequence of concern. To meet this requirement, the licensee should develop detection functions consistent with the controls described in the appendices. Note that the referenced controls are only applicable to VDAs. The detection functions should include data collection points and analysis mechanisms where technically feasible. These functions 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 detection functions 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 that 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, the monitoring of relevant threat intelligence resources, and lessons learned to improve early recognition of cyber attacks.

The licensee should use lessons learned from the detection or identification of new cyber security threats or attacks to inform and update, where applicable, their cyber security program. Acceptable detection functions identify abnormal activity on VDAs in a timely manner so that the licensee can respond, evaluate the potential impacts, and take compensatory measures if necessary. Detection also provides the CST information on the type of attacks occurring against the facility so that 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 use relevant threat intelligence sources to inform the detection functions (e.g., Government agencies, private cyber security organizations, or private industry data). The licensee should review the resulting data from the cyber security detection functions 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 licensee should review the detection functions, consistent with 10 CFR 73.53(g), to confirm its proper operation and should review its analysis efforts for accuracy. Overall, the licensee should seek to continuously improve its detection functions 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 protects 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. A licensee may 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 use various attack vectors (e.g., wired, wireless, or hand carried) to exploit unprotected VDAs. In addition, cyber attacks can be launched remotely, can occur over a broad timeframe, and could 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 necessary to determine which safety, security, and safeguards digital assets (if any) require protection against cyber attacks.

A licensee ensures that appropriate cyber security controls are maintained to protect VDAs in accordance with 10 CFR 73.53(d)(5). A licensee uses proper configuration and change management techniques when making alterations or updates to VDAs in accordance with 10 CFR 73.53(f). A licensee should assess plant changes to ensure the cyber security program performance objectives are maintained and determine whether 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 a consequence of concern.

This RG gives additional guidance on the cyber security protection required by 10 CFR 73.53 in Section C.3, for the CST; Section C.4, for the cyber security plan; Section C.5, for consequences of concern; Section C.6, for identification of digital assets; Section C.7, for cyber security controls; Section C.8, for implementing procedures and TCMs; Section C.9, for configuration management; Section C.10, for the review of the program; Section C.11, for event reporting and tracking; and Section C.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 responds to a cyber attack that is capable of causing a consequence of concern. Although the cyber security program is designed to protect against cyber attacks, exploits continue to be identified and evolve in both number and complexity. This makes completely impenetrable cyber security unrealistic. Therefore, effective and timely response to a cyber attack is important to minimize potential impacts. Given the nature of the cyber threat, a licensee should establish procedures and resources for response to cyber attacks that may exploit a VDA.

The licensee's response 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. These efforts remove the threat of cyber attack toward other VDAs and allow for eradication of potential malware. Finally, the licensee should preserve, where possible, all evidence of the attack for investigation. Section C.12 provides additional guidance on recordkeeping.

When a cyber attack is detected, the CST should confer with the safety, security, and safeguards 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. The licensee should take protective measures to prevent testing from introducing vulnerabilities. The licensee can prevent the introduction of vulnerabilities by testing systems before their installation, conducting tabletop exercises on critical systems, or evaluating software in "sandbox" (i.e., isolated) conditions. When testing identifies issues, they should be incorporated into the facility's corrective actions and, if appropriate, should 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. Section C.3 provides guidance on the CST's involvement in responding to a cyber attack.

After a licensee responds to a cyber attack and determines the resulting impacts of that attack, they should, if necessary, follow the specific event reporting and tracking requirements in 10 CFR 73.53(h). Section C.11 provides guidance on event reporting and tracking.

3 Cyber Security Team

As required by 10 CFR 73.53(d)(1), the licensee establishes 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 licensee should ensure that the CST:

a. protects VDAs and associated support systems from cyber attacks capable of causing a consequence of concern;

b. configures, operates, and maintains cyber security equipment to both detect and protect against a cyber attack capable of causing a consequence of concern;

c. 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;

d. 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;

e. conducts security audits, vulnerability assessments, network scans, table-top simulations, or penetration tests against VDAs where technically feasible without compromising the system;

f. authorizes VDAs for its use and assigns individuals to fulfill specific roles and responsibilities for this authorization process;

g. manages, documents, and reports the security state of VDAs;

h. assesses cyber threat intelligence and new vulnerability information;

i. conducts cyber security investigations following the compromise of VDAs;

j. preserves forensic evidence collected during cyber security investigations to prevent loss of evidentiary value;

k. creates a trained and qualified cyber security workforce through ongoing professional development;

l. maintains appropriate skills and knowledge in the area of cyber security;

m. performs duties with independence from the facility's operations, using well-defined responsibilities and sufficient authority to carry out those responsibilities;

n. performs, in part, as a cyber security incident response team (CSIRT);

o. provides role-related cyber security training and awareness to licensee staff members associated with VDAs; and

p. supports the cyber security configuration management system in accordance with 10 CFR 73.53(f).

The CST is a permanent unit within the licensee's organization. The number of individuals that comprise the CST may fluctuate over time and is expected to be scalable to the number of VDAs at a FCF. For example, during initial implementation of the cyber security program, contract employees may be needed to facilitate the identification of digital assets and development of the initial implementing procedures. If at that time a small number of VDAs are identified, staffing on the CST may be reduced to a level capable of maintaining the cyber security program performance objectives. Although 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 that these individuals have appropriate technical qualifications and are deemed trustworthy for their authorized role on the team.

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

The CST should also consider how VDAs are authorized to operate after controls are addressed and verified as a result of changes to the licensee's environment or digital assets. The cyber security program manager or program sponsor should have a role in this process. This would include incorporating

and validating changes to documentation or other implementing procedures to reflect adjustments to cyber security controls or their associated measures. In addition, the VDA authorization process itself should be incorporated in licensee procedures.

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). The NRC would find the following four categories of individuals acceptable for administering an effective cyber security program:

a. Cyber Security Program Sponsor. This individual provides oversight as a member of senior site management (executive level) and is overall accountable for the cyber security program. Some of their additional responsibilities may include, but are not limited to: ensuring the cyber security program objectives and requirements are correctly prioritized, scheduled, resourced, and budgeted; approving key cyber security deliverables and policies; resolving conflicts and issues beyond the control of the Cyber Security Program Manager; and acting as a link between the cyber security program and overall business and operations.

b. Cyber Security Program Manager. This individual is responsible for coordinating, developing, implementing, and maintaining the cyber security program and provides oversight and direction to the CST. The individual serves as the single point of contact between upper management and the CST and is overall responsible for the identification and protection of VDAs. Some of their additional responsibilities may include, but are not limited to: development, implementation and maintenance of the cyber security plan; implementing and maintaining a cyber security incident response capability and configuration management system; conducting vulnerability assessments; developing and maintaining a cyber security budget; and monitoring the cyber security program to ensure performance objectives are met and maintained.

c. Cyber Security Specialist. This individual is responsible for the day-to-day implementation, maintenance and monitoring of the cyber security program. The individual is responsible for providing technical expertise and guidance to the technical staff members for implementation of the cyber security program and protection of VDAs. Some of their additional responsibilities may include, but are not limited to: developing and maintaining cyber security implementing procedures and ensuring VDAs are protected consistent with the cyber security plan; monitoring VDAs and cyber security controls for degradations, vulnerabilities and compromise; performing vulnerability scans, auditing logs and monitoring for cyber attacks; testing, configuring and installing security software, patches and hardware as needed (e.g., firewalls, network or host intrusion detection, etc.). The number of Cyber Security Specialists may vary based on the number of VDAs.

d. Technical Staff Members. Technical staff members from facility organizations, including security, operations, engineering, material control and accounting, and other support organizations (as required), are responsible for maintaining alternate means to address digital assets associated with a consequence of concern. Some of their additional responsibilities may include, but are not limited to: assisting with the development and maintenance of implementing procedures and monitoring VDAs and cyber security controls within their technical area. These staff members

may or may not be part of the CST, but they provide technical input on the analysis of digital assets and protection of VDAs.

The cyber security plan summarizes the team's organizational structure in accordance with 10 CFR 73.53(i).

3.2 Training and Qualifications

The licensee ensures 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 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 requirements for the CST should be documented in the cyber security plan. The training should include initial and recurring annual training requirements. In addition, completion of the initial and recurring training for each individual on the CST should be documented and maintained. The licensee should keep records to indicate each individual's type of training received commensurate with their roles and responsibilities on the CST. Additional training requirements may be necessary to ensure familiarity with the implementation and monitoring of cyber security controls and protection of VDAs.

Qualifications

The licensee should establish and document minimum qualification requirements for each key position on the CST. The individual's qualifications should be documented, maintained and available for review. The cyber security program sponsor should have general knowledge, training or experience working in cyber security. The cyber security program manager should have experience, training or education that provides him or her the knowledge, skills and abilities to effectively develop and maintain a cyber security program consistent with the program performance objectives and requirements. The cyber security specialist should have experience, training or education that provides him or her the knowledge, skills and abilities to effectively implement, maintain and monitor a cyber security program consistent with program performance objectives and requirements. The technical staff members who support the CST should have experience and knowledge of the digital assets used throughout their technical area of operations. These individuals should not perform their assigned duties and responsibilities until they are properly trained and qualified.

3.3 Equipment

The licensee should provide the CST with the appropriate software, tools, and devices to analyze networks and related traffic, scan devices to verify that 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 and the latest information from common vulnerabilities and exposures compatible databases (e.g., the National Cybersecurity Federally Funded Research and Development Center, U.S. Department of Homeland Security Industrial Control Systems, and U.S. Department of Homeland Security Cyber Emergency Response Team).

4 Cyber Security Plan

As required by 10 CFR 73.53(e), a licensee establishes, implements, and maintains a site-specific cyber security plan that describes how the licensee satisfies 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 and 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 are used to protect against cyber attacks capable of causing the consequences of concern. Under 10 CFR 73.53(a), the licensee incorporates the cyber security plan 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 address technical (e.g., network infrastructure); physical (e.g., digital assets used at the FCF); 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.

The licensee should include in their cyber security plan their goals for addressing cyber security in their daily operations for protection of VDAs. The licensee 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 that 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 onsite for the implementation of the cyber security program. In addition, the cyber security plan should describe how the licensee identifies, evaluates, and protects 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

Appendix A to this RG provides a generic cyber security plan template the licensee can use to guide the development of a cyber security plan that complies with the requirements of 10 CFR 73.53(a) and (e).

As required by 10 CFR 73.53(e), the cyber security plan describes how the licensee detects, protects against, and responds to a cyber attack capable of causing a consequence of concern identified in 10 CFR 73.53(c). The cyber security plan addresses the following elements:

a. documentation that the CST is established and maintained in accordance with 10 CFR 73.53(d)(1), including sufficient detail to demonstrate that the CST is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program;

b. description of the cyber security controls and associated performance specifications for which measures are taken to prevent a cyber attack from causing a consequence of concern, as required by 10 CFR 73.53(d)(2);

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

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

e. description of the process for taking measures to address the performance specifications of the identified cyber security controls for VDAs to ensure protection against a cyber attack capable of causing a consequence of concern, as required by 10 CFR 73.53(d)(5), including a description of the process to:

(1) determine the measures (e.g., physical hardware, software, and activities) for meeting the parameters of the applicable cyber security controls;
(2) justify instances when measures are not applied to certain VDAs and document how equivalent protection is achieved; and
(3) establish and maintain written implementing procedures (outside of the cyber security plan) for these measures and justifications.

f. description of how TCMs 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 to meet the cyber security program performance objectives, as required by 10 CFR 73.53(d)(6);

g. 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), including sufficient detail to demonstrate that these changes are evaluated before their 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);

h. description of the periodic review process to be used to evaluate the cyber security program, as required by 10 CFR 73.53(g), including sufficient detail to demonstrate how the licensee evaluates the effectiveness and adequacy of the program and controls, alternate means used, defensive architecture for digital assets, and the related implementing procedures and how the results are addressed, tracked, and reported as required;

i. description of measures for cyber security incident response (CSIR) to a cyber attack that affects VDAs or that may cause a consequence of concern, including event reporting and tracking as required by 10 CFR 73.53(h);

j. description of how a fully implemented cyber security program is maintained and managed, as required by 10 CFR 73.53(b) and 10 CFR 73.53(e)(1)(ii), respectively;

k. summary descriptions of cyber detection activities planned for use by the licensee;

l. confirmation that the licensee meets the reporting requirements in 10 CFR 73.53(h), referencing the log to be used for recordable events in accordance with 10 CFR 73.53(h)(2); and

m. confirmation that the licensee meets the recordkeeping requirements in 10 CFR 73.53(i), including the title for the position managing the records associated with 10 CFR 73.53 and the cyber security program.

Consistent with 10 CFR 73.53(e)(2), the 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, should not be submitted to the Commission for review and approval as part of the cyber security plan, however this information is 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 as a result of applicable changes in VDAs as part of the 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 require NRC review and approval in accordance with 10 CFR 40.32(h) or 10 CFR 70.32(f), whichever regulation applies to the specific licensee before implementation of the change.

A cyber security plan should describe the resources and governing procedures to ensure that cyber security information, associated records, and implementing policies and procedures are appropriately evaluated for protection of Safeguards Information, in accordance with 10 CFR Part 73, and protection of classified information, in accordance with 10 CFR Part 95. Revisions to the cyber security plan are processed in accordance with 10 CFR 40.32(h) or 10 CFR 70.32(f), whichever is applicable to the specific licensee. A licensee submits changes that would result in a decrease in the effectiveness of the cyber security plan to the NRC for review and approval before their implementation.

4.2 Managing the Cyber Security Program

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

Once the program is fully implemented, the licensee maintains the cyber security program as required by 10 CFR 73.53(b). The licensee should maintain the program through effective management of personnel, resources, and established activities. This management should oversee and develop the CST. In turn, the CST performs the regular or periodic duties and activities necessary to meet the performance objectives of and the specific performance specifications for cyber security controls associated with VDAs.

The NRC expects management of the fully implemented cyber security program to reflect the following concepts:

a. 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 and 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.

b. 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 develops from the lessons learned of previous activities, information shared by other sources, and continuous awareness of activities associated with VDAs and the threats to their cyber security.

The NRC expects the licensee to adjust their management practices as necessary to maintain the effectiveness of the cyber security program, including making changes to reflect the recommendations stemming from the periodic review required by 10 CFR 73.53(g) and incorporating lessons learned from the CSIR capability.

4.3 Cyber Security Incident Response

A licensee's cyber security plan describes the measures taken to respond to a cyber attack capable of causing a consequence of concern in accordance with 10 CFR 73.53(e)(2)(iii). This information is 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 maintained with current information. 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 responds to a cyber attack capable of causing a consequence of concern. To satisfy this requirement, the licensee 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 its 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 the 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 whether 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 essential services (e.g., power, lighting, heating, ventilation, and air conditioning) exists. The licensee should plan to maintain vital 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 personnel 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.

The licensee follows the specific event reporting and tracking requirements in 10 CFR 73.53(h). Section C.11 provides guidance on event reporting and tracking. The licensee should also incorporate lessons learned into CSIR procedures, training, and testing. These lessons learned may also require changes to the CSIRP. 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 in accordance with 10 CFR 73.53(g). The exercise itself should be as realistic as practicable 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 and into the overall CSIRP and related procedures.

4.4 Emergency Plan

A licensee is required to address the emergency plan requirements in accordance with 10 CFR 40.31(j) or 10 CFR 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 activates the emergency plan, the emergency plan would be used to respond to the event even if it involved a cyber attack. The licensee should use the CSIRT to respond to cyber attacks that do not involve, or have not yet involved, the emergency plan. The CSIRT may also serve as a resource for implementing the emergency plan if necessary; however, in these cases, it should be made clear that the CSIRT would be using emergency plan procedures, not the CSIRP.

5 Consequences of Concern

As required by 10 CFR 73.53(c), a licensee's cyber security program is designed to protect against the specified consequences of concern that are appropriate to the facility type of the licensee. Table C-1 describes the consequences of concern and compiles the associated regulatory thresholds. The consequence of concern thresholds were informed by: the safety regulations in 10 CFR Part 70; security requirements in 10 CFR Part 73 and 10 CFR Part 95; and material control and accounting requirements in 10 CFR Part 74.

The NRC is seeking to protect licensed activities that have the potential for a cyber attack to cause or result in any of the following consequences of concern, as specified in 10 CFR 73.53(c). By targeting these consequences, the NRC expects a licensee to focus its cyber security efforts to effectively protect against cyber threats associated with risk-significant impacts.

Table C-1. Consequences of Concern and Related References

TYPE 1: LATENT – DESIGN-BASIS THREAT The compromise, as a result of a cyber attack at a FCF authorized to possess or use a formula quantity of strategic SNM, of a function needed to prevent one or more of the following:	
a. radiological sabotage;	Informed by: 10 CFR 73.1(a)(1)
b. theft or diversion of formula quantities of strategic SNM; or c. loss of nuclear material control and accounting for strategic SNM.	Informed by: 10 CFR 73.1(a)(2) 10 CFR 73.20 10 CFR 74.51
TYPE 2: LATENT – SAFEGUARDS The compromise, as a result of a cyber attack at a FCF authorized to possess or use SNM of moderate strategic significance, of a function needed to prevent one or more of the following:	
a. unauthorized removal of SNM of moderate strategic significance; or b. loss of nuclear material control and accounting for SNM of moderate strategic significance.	Informed by: 10 CFR 73.67 10 CFR 74.41
TYPE 3: ACTIVE – SAFETY One or more of the following that directly results from a cyber attack:	
a. radiological exposure of 0.25 Sv (25 rem) or greater for any individual; b. 30 milligrams or greater intake of uranium in soluble form for any individual outside the controlled area; or c. an acute chemical exposure that could lead to irreversible or other serious long-lasting health effects for any individual.	Informed by: 10 CFR 70.61 and 10 CFR 70.62
TYPE 4: LATENT – SAFETY AND SECURITY The compromise, as a result of a cyber attack, of a function needed to prevent one or more of the following:	
a. radiological exposure of 0.25 Sv (25 rem) or greater for any individual; b. 30 milligrams or greater intake of uranium in soluble form for any individual outside the controlled area; c. an acute chemical exposure that could lead to irreversible or other serious long-lasting health effects for any individual; or	Informed by: 10 CFR 70.61 and 10 CFR 70.62
d. loss or unauthorized disclosure of classified information or classified matter.	Informed by: 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 a licensee addresses through its cyber security program: latent – DBT (Category I FCF licensees only), latent – safeguards (Category II FCF licensees only), active – safety, and latent – safety and security:

a. A latent – DBT consequence of concern can only occur at a FCF authorized to possess or use a formula quantity of strategic SNM (i.e., Category I FCF licensee). The latent – DBT consequence of 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 SNM, or the loss of nuclear material control and accounting for the aforementioned nuclear material. A latent consequence of concern

for the DBT potentially prevents a licensee from meeting the requirements of 10 CFR 73.1(a)(1), 10 CFR 73.1(a)(2), or 10 CFR Part 74.51 during a secondary event.

b. A latent – safeguards consequence of concern can only occur at a FCF authorized to possess or use SNM of moderate strategic significance (i.e., Category II FCF licensee). Similar to the latent – DBT consequence of concern, a latent – safeguards 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 SNM of moderate strategic significance.

c. 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. This manipulation can be intentional on the part of the attacker or unintentional.

d. A latent – safety or security consequence of concern has the potential to occur at any FCF licensee, although the security element would only be applicable to a licensee who possesses classified information or matter. 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 their intended safety or security functions. When called upon to respond as a result of 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 occurs.

Licensees should be aware of several distinct differences between the 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. In the latent case, a function is compromised, but there is no immediate 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 the secondary event (e.g., process hazard initiating event or physical attack). The combination of the compromise from the cyber attack, the resulting latent consequence of concern, and the secondary (i.e., initiating) event would need to occur for there to be an 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 may elapse 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. For this reason, robust detection and response capabilities are important aspects of an adequate cyber security program. Conversely, the cyber security controls and response efforts for active consequences of concern should account for a compromise that can directly cause a consequence of concern. For this reason, robust protection is an important aspect of an adequate cyber security program because the time for response may be limited.

The licensee should use the types of consequences of concern listed in Table C-1 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 consequences of concern depend on the facility classification as follows:

a. Conversion and deconversion FCF licensees would consider the following:

(1) active – safety; and
(2) latent – safety and security.

b. Category III FCF licensees would consider the following:

(1) active – safety; and
(2) latent – safety and security.

c. Category II FCF licensees would consider the following:

(1) active – safety;
(2) latent – safety and security; and
(3) latent – safeguards.

d. Category I FCF licensees would consider the following:

(1) active – safety;
(2) latent – safety and security; and
(3) latent – DBT.

A licensee should consider the possibility that a digital asset may be associated with more than one consequence of concern. Section C.6 provides additional guidance on the identification of digital assets and VDAs. Section C.7 provides additional guidance on addressing the performance specifications of cyber security controls.

6 Identification of Digital Assets

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

a. Step 1. Identify digital assets associated with consequences of concern.
b. Step 2. Identify VDAs by considering alternate means.
c. Step 3. Determine boundary and support systems for each VDA.

6.1 Identifying Digital Assets Associated with a Consequence of Concern

As required by 10 CFR 73.53(d)(3), a licensee identifies digital assets that, if compromised by a cyber attack, would result in a consequence of concern. The glossary to this document defines a digital asset as an electronic device, or organized collection of devices, that processes information, communicates data, or is 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, in accordance with the requirements of

10 CFR 73.53(d)(3), a licensee does not need 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.

To develop an effective protection strategy, the licensee compiles in-depth knowledge of how digital assets affect their site operations that are associated with a consequence of concern. To gain this knowledge, a licensee should do the following:

a. Identify site areas and processes associated with a consequence of concern.

b. 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).

c. Examine those functions and identify the role of digital assets.

d. Determine whether the compromise of the digital asset would directly lead to a consequence of concern (i.e., active – safety). Additionally, determine whether 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, a licensee should review:

    (1) software platforms and applications related to digital asset functions or processes; and
    (2) communication and data flow involving the digital asset.

If the compromise of the digital asset would lead to one or more of the consequences of concern, the digital asset is within the scope of 10 CFR 73.53 and requires further analysis to determine whether it is vital.

The Cyber Security Plan may describe a generic identification process for digital assets. Appendix G provides an example of applying a generic identification process. A licensee should, at a minimum, use the following resources to support the identification process:

a. integrated safety analyses or process hazards analyses (or both);

b. security plans (e.g., Standard Practice and Procedures Plan, Physical Security Plan, Information Security Plan, or Safeguards Contingency Response Plan);

c. fundamental nuclear material control plan;

d. security orders;

e. previously considered impacts from a cyber attack;

f. site or system vulnerability analyses; or

g. other safety or security information.

Digital assets associated with consequences of concern may exist as part of a number of safety and security programs throughout the facility. Examples of systems that may contain digital assets related to the consequences of concern include the following:

a. items relied on for safety – potential active or latent safety consequences of concern;

b. plant features and procedures – potential active or latent safety consequences of concern;

c. intrusion detection systems (physical security) – potential latent security (for protection of classified information or matter), safeguards, or DBT consequences of concern; and

d. material control and accounting database – potential latent safety, safeguards, or DBT consequences of concern.

The licensee identifies digital assets that, if compromised by a cyber attack, would result in a consequence of concern as required by 10 CFR 73.53(d)(2). A licensee should document the following information (e.g., in a table or list) to identify all digital assets associated with a consequence of concern:

a. the name and physical location of the application, device, system, or network identified as a digital asset; and

b. which of the four types of consequences of concern potentially apply if a compromise of the digital asset were to occur.

In accordance with 10 CFR 73.53(e)(2), the licensee does not submit a site-specific analysis and other supporting technical information used to develop and implement the cyber security plan to the Commission for review and approval, but this information is subject to NRC inspection. As required by 10 CFR 73.53(i), a licensee retains the supporting documentation demonstrating compliance with the requirements of 10 CFR 73.53 as a record.

6.2 Alternate Means Analysis

After a licensee identifies those digital assets associated with a consequence of concern, the licensee determines which of those digital assets are vital as required by 10 CFR 73.53(d)(4). This analysis determines whether 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 protecting the digital asset in lieu of cyber security controls. A licensee should consider the function of the digital asset to determine whether an alternate means exists that could be credited or implemented to prevent the consequence of concern.

When considering options during this analysis, the licensee should identify acceptable alternate means having the following attributes:

a. are protected from a cyber attack;

b. are sufficiently reliable and adequately implemented consistent with other safety or security features;

c. are properly maintained and periodically tested;

d. prevent the identified consequence of concern;

e. can be activated in a timely manner to prevent the identified consequence of concern;

f. would be implemented with available resources;

g. would not be adversely impacted by the potential multi-node effects from a cyber attack;

h. consider the cumulative effects from a cyber attack; and

i. do not contribute to other vulnerabilities or lead to a consequence of concern.

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

a. physical barriers;

b. material holding tanks;

c. temperature, pressure, and volume regulators or sensors;

d. flow control of material through the production process;

e. items relied on for safety (similar to plant features and procedures at some licensees);

f. process monitoring equipment and procedures;

g. failsafe features or processes;

h. other VDAs; or

i. manual actions (e.g., administrative IROFS or routine security patrols) that are performed which are redundant to the functions being analyzed.

The licensee may credit a single, acceptable alternate means for multiple digital assets to prevent a consequence of concern. Multiple digital assets may share an acceptable alternate means if the licensee has considered the potential cumulative effects from simultaneous compromise of the associated digital assets.

The licensee should consider factors that 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 perform the function of several digital assets simultaneously. Rather, the licensee could demonstrate that multiple attack vectors are not feasible.

Crediting a manual action as an acceptable alternate means should only be done after determining that the action is reliable. The compromise of a function by a cyber attack is extremely difficult to detect and should not be relied upon to initiate a manual action (i.e., reactive actions are generally not acceptable alternate means). However, preventative manual actions (e.g., process stoppage in a timely manner before the consequence of concern can occur) may be credited if the following are considered:

a. environmental factors (e.g., lighting, radiation levels, or temperature) that could affect the action;

b. notification and equipment with the necessary functionality and accessibility to perform the action;

c. indication and confirmation of the expected result;

d. procedures and training for the action;

e. adequate staffing to perform the action; and

f. demonstration (e.g., testing) of the action.

The licensee should develop an analysis for crediting a resource as an alternate means. The licensee should ensure that the alternate means prevents the consequence of concern. A generic process for analyzing the adequacy of potential alternate means should be provided in the cyber security plan. Appendix G provides an example description of a generic alternate means analysis. On-site documentation of the alternate means analysis should include, at a minimum, a brief description of any alternate means credited for a digital asset and the applicable characteristics that make the alternate means acceptable. The documentation associated with the analysis of alternate means 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, standalone, or protection by a firewall, data diode, virtual local area network, tunneling, or cross-domain solution), these characteristics alone do not provide 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, and other such features); plant procedures; and other physical security activities that do not address all cyber attack vectors.

The design and configuration of a digital asset may, however, provide measures that address certain performance specifications of the cyber security controls. To take credit for the security features of the existing design and configuration, a licensee documents them as discussed in Section C.7.2.

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). Section C.7.2 provides additional information on addressing the performance specifications of cyber security controls.

6.2.1 Consideration of air-gapped digital assets

Air-gapped digital assets are not physically connected to a network or to other digital systems. To be considered “air-gapped”, a digital asset is standalone with no communications capability, enforced by physical or hardware means. The functions performed by an air-gapped digital asset are unable to be compromised through a network-based cyber attack. The physical or hardware enforcement of communication capability is necessary to prevent the modification of software or configuration settings that could allow unauthorized or unintended network communications. This could occur through system maintenance activities, operator error, or system compromise (e.g., portable media).

The presence of an air-gap does not exempt a digital asset from further analysis, as it does not address all cyber attack vectors. However, an air-gap is a measure that addresses certain performance specifications of the cyber security controls. To take credit for the security features of an air-gap, a licensee documents them as discussed in Section C.7.2.

6.2.2 Consideration of digital assets and data diodes

A data diode is a deterministic optical/electronic network device that permits the flow of communications in one direction only. This is enforced through physically preventing electron flow in one direction. The directionality of the communications in a data diode cannot be altered through software, configuration, or operator action. Communication directionality may only be altered through significant physical manipulation of the device or the wiring. A digital asset is considered separated from the network by a data diode if the communications from the digital asset is allowed to traverse the data diode and travel to systems and networks isolated by the data diode, but communications to the digital asset from systems outside the path established by the diode is prevented by the optical/electronic barrier posed by the diode. The digital asset may still be able to communicate with other digital systems located on the same side of the data diode, but the location of the data diode is considered when determining if cyber security controls addressing network-based threats and attack pathways are fully addressed by the data diode. Additionally, the licensee has demonstrated that all communication with the isolated systems flow through the data diode and that no other communications methods (e.g., wireless networking or modems) exist that are not similarly controlled. A digital asset behind a data diode can be said to be unreachable using remote access methods over the wired network.

The presence of a data diode does not exempt a digital asset from further analysis, as it does not address all cyber attack vectors. Note that other methods of access (e.g., wireless) are not inherently addressed by the data diode. However, a data diode is a measure that addresses certain performance specifications of the cyber security controls. To take credit for the security features of a data diode, a licensee documents them as discussed in Section C.7.2.

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. VDAs are protected from cyber attack by addressing the performance specifications of the appropriate cyber security controls. Written implementing procedures are created to establish and maintain the measures taken to address the cyber security controls in accordance with 10 CFR 73.53(d)(5).

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 (i.e., within a common boundary) between 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 and are considered if their compromise by a cyber attack could lead to a consequence of concern. Examples of support systems include, but are not limited to: electrical power; heating, ventilation, and air conditioning; communications; and fire suppression. Sections C.6.3.1 and C.6.3.2 provide additional guidance on VDA boundaries and support systems.

For a VDA associated with more than one consequence of concern, a licensee should address the most comprehensive cyber security controls that apply. Section C.7 provides additional guidance on addressing the performance specifications of cyber security controls.

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

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

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

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

Section C.8 provides additional guidance on VDA documentation and the associated cyber security control implementing procedures.

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 controls. 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 scope for taking the measures to address the performance specifications of the appropriate cyber security controls. The VDA's boundary definition should be documented and this documentation is subject to inspection by the NRC in accordance with 10 CFR 73.53(e)(2).

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, and smart phones). A licensee should consider the level of dependence between the VDA and its support systems to determine whether a compromise of the support system could do the following:

a. provide an input to a VDA that causes a consequence of concern;

b. directly cause a consequence of concern; or

c. preclude the VDA from performing the function needed to prevent a consequence of concern.

If any of the three conditions above apply, the licensee protects the identified support system from a cyber attack capable of resulting in a consequence of concern, in accordance with 10 CFR 73.53(d)(5). 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, the licensee should address the more comprehensive cyber security controls specific to the applicable consequences of concern. Section C.7 provides additional guidance on addressing the performance specifications of cyber security controls.

6.3.3 Grouping of Vital Digital Assets

VDAs may be grouped to more efficiently address cyber security controls, provided the controls can be applied equally to address the associated consequences of concern. Grouping similar VDAs (e.g., programmable logic controllers, distributed control systems, supervisory control, and data acquisition) may improve efficient application of controls. This is commonly referred to as "type accreditation" for NIST-style authorizations.

When similar VDAs are grouped, one implementing procedure may be applied to the entire group to facilitate documenting the measures taken to address the performance specifications of the cyber security controls. In addition, the licensee should evaluate the boundary for each VDA throughout the group. The documentation associated with the digital asset identification process should note the grouping of the VDAs. In accordance with 10 CFR 73.53(e)(2), this documentation is subject to inspection by the NRC.

7 Cyber Security Controls

A cyber security control contains 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. The performance specification of a cyber security control is satisfied by taking measures to address the cyber attack capable of causing a consequence of concern. To effectively protect VDAs against cyber attacks associated with a consequence of concern, a licensee establishes and maintains cyber security controls as required by 10 CFR 73.53(d)(2). In accordance with 10 CFR 73.53(d)(5), a licensee takes measures and documents such measures to address the performance specifications of the appropriate cyber security controls. As required by 10 CFR 73.53(e)(1), the licensee's cyber security plan documents cyber security controls for the specific types of consequences of concern.

7.1 Standards and Applicable Cyber Security Controls

The licensee's cyber security plan should identify the guidance or standard(s) that the licensee uses to establish and maintain cyber security controls (e.g., this regulatory guide, NIST, or ISO/IEC). The controls are subject to NRC review for acceptance in accordance with 10 CFR 73.53(d)(2). The licensee documents the cyber security controls in its cyber security plan, similar to the example provided in Appendix A to this document.

7.2 Establishing Cyber Security Controls and Addressing Performance Specifications

In accordance with 10 CFR 73.53(d)(3) and (4), the licensee determines the type of consequence of concern that could result if each VDA is compromised. As required by 10 CFR 73.53(d)(5), a licensee ensures each VDA is protected against a cyber attack by taking measures to meet performance specifications for the appropriate cyber security controls. These measures are documented in the associated implementing procedures for each VDA. To satisfy this requirement, the licensee can use the controls listed in the appendices in 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). Alternatively, a licensee may use equivalent controls derived from other sources (e.g., NIST or ISO/IEC) if the sets of controls are recorded in the NRC approved cyber security plan (see discussion on other sources of information in Section B). The licensee should document how it addresses these controls in the implementing procedures for the VDAs. The documentation should demonstrate that the controls are adequate to prevent the consequence of concern. Section C.8 provides additional guidance on implementing procedures.

The NRC has developed the following cyber security controls for use by FCF licensees:

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

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

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

d. 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

e. 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, it should address each cyber security control applicable to the type of consequence of concern associated with each VDA.

If the licensee submits a different set of controls for NRC approval, in accordance with 10 CFR 73.53(d)(2) and (e)(1), the licensee:

a. develops cyber security controls specific to the applicable types of consequence of concern;

b. establishes the performance specifications of the controls to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern; and

c. documents the controls in the cyber security plan.

Appendix B contains cyber security controls that are applicable to all VDAs, whereas Appendices C–F are graded based on the consequence of concern. The appendices, in order by decreasing comprehensiveness of cyber security controls, are: (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 NRC expects it to use the more comprehensive cyber security controls when more than one consequence of concern is possible for a VDA.

This graded comprehensiveness should be present if a licensee submits a different set of controls for NRC approval. In this case, when more than one consequence of concern is possible for a particular VDA, the licensee addresses the controls for all applicable consequences of concern for that VDA from the more comprehensive control set.

The licensee can address the performance specification of a cyber security control by taking measures to detect, protect against or respond to a cyber attack capable of causing a consequence of concern. A measure is a capability, item, or action (e.g., computer hardware, software, and plant procedures) that provides protection from a cyber attack vector and is taken to address 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.

The licensee should recognize that each control is 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 73.53(d)(2) and documented in the cyber security plan. The type(s) of consequence(s) of concern associated with the VDA under consideration determine the cyber security controls that the licensee addresses. In accordance with 10 CFR 73.53(d)(5) and (e)(2), the licensee documents how it addressed each cyber security control in the implementing procedure associated with the VDA and maintain those records 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 its justification for not taking measures in the implementing procedure for the VDA. 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) and operational choices by the licensee (e.g., media protection is not required because 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. A licensee who submits unique sets of cyber security controls for NRC approval should clearly define and record similar parameters. These parameters should be documented in the definitions of the controls and made available 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 (i.e., 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. The licensee should account for and address every control established for the applicable consequence of concern. If certain cyber security controls are tailored, the associated rationale should be recorded in the implementing procedures (or references to other relevant documentation should be 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 a licensee to credit controls already in place for related assets or group of 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. The use of common controls for all VDAs or certain groups of VDAs may reduce the administrative effort in satisfying controls and developing implementing procedures. It is up to the licensee to determine, based on site specific characteristics, where common controls and their associated measures can be used. The NRC expects 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, the NRC expects that the appropriate implementing procedures would document inherited controls to provide traceability to the parent VDA where the control is originally applied.

7.3 Verifying Cyber Security Controls

After 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 that documents the measures taken to address the performance specifications for the controls applicable to each VDA should describe the conditions under which this assessment is conducted, the frequency of the assessment, and roles and responsibilities for the team conducting the assessment. The licensee should document the results in the associated implementing procedure and make 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, for each interconnection, the NRC expects the licensee, through its cyber security program, to analyze and document the interface characteristics, security requirements, and 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 CST should review the results of the controls and VDA assessments. If the assessments show that all controls have been effectively implemented, the cyber security 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 through an assessment. Otherwise, the licensee can also choose to use a TCM to operate the VDA until the required solution can be reworked and assessed.

7.4 Cyber Security Control Maintenance

The licensee should maintain cyber security controls as a part of their overall cyber security program so that they remain applicable to existing conditions at the FCF. The licensee should develop new cyber security controls, control enhancements, or modifications to existing controls as needed based on the latest state-of-the-practice information from national-level threat and vulnerability databases and 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, the licensee submits any additions, modifications, or changes that would result in a decrease in the effectiveness of a cyber security control to the NRC in accordance with 10 CFR 40.32(h) or 10 CFR 70.32(f), whichever regulation applies to the specific licensee, for review and approval before their implementation.

8 Implementing Procedures and Temporary Compensatory Measures

Consistent with the requirements in 10 CFR 73.53(d)(5)(ii), the licensee establishes and maintains 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. Appendix G provides an example of an implementing procedure.

In accordance with 10 CFR 73.53(d)(6), a licensee implements TCMs when the measures taken to address the performance specifications of the controls fail to meet the cyber security program performance objectives. The licensee should document and track the TCMs to completion when used to protect a VDA.

8.1 Implementing Procedures

Implementing procedures identify and document the cyber security controls applicable to the VDA(s). A licensee may reference existing procedures to avoid redundancy, like in the case of common controls. At a minimum, the implementing procedures should document the information described below.

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, and 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 whether 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 Vital Digital Asset

The procedure should identify the individual(s) by job title or role (e.g., security manager) or organization (e.g., licensee's 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 and communications protocol). The procedure should include a network diagram showing the VDA's interconnections and defined boundaries. The licensee 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. Section C.6.3.2 contains additional information. The procedure should describe the VDA's reliance on the support system. If the support system is identified as a separate VDA, 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 should do one of the following:

a. take new measures to meet the performance specifications outlined in the control;

b. use existing measures to meet the performance specifications outlined in the control; or

c. justify that the control is not applicable to the VDA.

If the licensee determines that a new measure is required, it should evaluate the control to identify the performance specification and seek CST confirmation that the identified measure satisfies the performance specification needed to protect the VDA. Once the licensee has confirmed the measure, it should develop and document the measure's expected performance in the implementing procedure. The licensee should ensure the performance of proper configuration management. When taking new measures,

the licensee should validate cyber security controls through testing (e.g., vulnerability scanning and tabletop exercises).

If the licensee determines an existing measure is used, it should evaluate the control to identify the performance specification. The CST should confirm the existing measure satisfies the performance specification needed to protect the VDA. Once the licensee has confirmed the measure, it should develop and document through reference the existing measure's expected performance in the implementing procedure. When using existing measures, cyber security controls are validated through confirmation of their applicability to the VDA.

If the licensee determines that a control is not applicable, it should 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 the licensee provides 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. The implementing procedure should reference or describe the grouping of VDAs, as noted in the documentation associated with the digital asset identification process.

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 appropriate implementing procedures should reference the use of common or inherited controls.

8.2 Temporary Compensatory Measures

If after an implementing procedure has been completed and the intended measure does not meet the performance specifications of the control, a licensee may implement TCMs in accordance with 10 CFR 73.53(d)(6). A TCM is an interim solution to replace a measure(s) used to address one or more cyber security controls and the associated performance specifications. In lieu of shutting down and securing the VDA, a TCM is a time-limited solution that allows the VDA to be operated while the long-term method to address the control is properly implemented and verified. Documenting and tracking the TCM allows the licensee to verify its completion.

The licensee should document the function of the TCM, how it effectively addresses the control, and a timetable for the interim measure. The licensee should document, at regular intervals, progress on implementing a long-term solution and ensure that the issue is tracked to completion. The licensee should document a justification and have internal management approval for a TCM that would be kept in use for more than 1 calendar year from the date of its adoption.

A TCM is employed, as necessary, for a VDA if a measure fails 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 by 10 CFR 73.53(f) may identify new or modified measures implemented through procedures, which may require a TCM or shutdown of the

VDA. Furthermore, the periodic review process required through 10 CFR 73.53(g) may identify findings, deficiencies, and recommendations that may require TCMs.

9 Configuration Management

After a licensee has fully implemented the cyber security program by identifying and protecting its VDAs, the licensee implements a configuration management system to ensure that changes to the facility are properly evaluated in accordance with 10 CFR 73.53(f). This system ensures that changes (e.g., addition, modification, or removal of devices and equipment) are evaluated before their implementation and that they do not adversely impact the licensee's ability to meet the cyber security program objectives. The licensee documents this system in written procedures and can add it 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 be done through 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 the licensee 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 whether 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 whether the proposed change would affect or degrade existing alternate means and measures taken to address cyber security controls. Additionally, this impact analysis would determine whether adjustments would be required to maintain the effectiveness of the existing detection functions or implementing procedures. Furthermore, this impact analysis would consider the potential effects that the proposed change would have on the cyber security plan, CSIR procedures, other documentation, or processes.

Before making a design or configuration change to a VDA or when changes to the environment occur, a licensee should, at a minimum, 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 when technically

feasible. 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. TCMs can be employed, as needed, if the new implementing procedure proves inadequate.

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 and 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 performs a review of its cyber security program. The periodic review serves to evaluate the overall effectiveness of the cyber security program. A licensee authorized to possess or use a formula quantity of strategic SNM performs a review of the cyber security program as a component of the security program in accordance with 10 CFR 73.46(g)(6), including the periodicity requirements. All other licensees perform a review of the cyber security program at least every 36 months. This requirement, derived from the 24 month programmatic review required by power reactors in 10 CFR 73.54, was informed based on the hazards associated with these FCF licensees.

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

a. purpose, scope, roles, responsibilities, requirements, and management support of the cyber security program;

b. changes made to implementing procedures;

c. measures of performance established through cyber security controls and whether the licensee developed, monitored, and reported on the results of these performance measures;

d. cyber security control strategy;

e. use of alternate means and defensive architecture for digital assets;

f. facility's CSIR capability;

g. configuration management system; and

h. 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 tracks; addresses in a timely manner; and documents 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 initiate changes to: (1) the cyber security plan; (2) the cyber security controls or alternate means; (3) the CSIR; or (4) the implementing procedures for VDAs and associated controls.

Consistent with 10 CFR 40.32(h) or 10 CFR 70.32(f), a change that would result in a decrease in the effectiveness to the cyber security plan, including the cyber security controls, is submitted to the NRC for review and approval before 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, a licensee informs the NRC Operations Center within 1 hour of discovery that an event requiring notification under existing regulations is the result of a cyber attack. Secondly, as required by 10 CFR 73.53(h), a licensee records certain events within 24 hours of their discovery and tracks them to resolution.

11.1 Event Reporting

A licensee informs 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 the licensee to initiate a separate report to the NRC; instead, a licensee 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.

Licensees should be prepared to provide the following information, if available, at the time of the notification:

a. caller name and callback number;

b. facility name and location;

c. emergency classification (if declared);

d. current event status (e.g., in progress, recovered);

e. event date and time (discovery of, and actual occurrence if known);

f. event description including cyber security controls involved/affected (if any), system(s) involved/affected (e.g., safety or security functions, digital asset, or VDAs), method used to identify the event (e.g., security controls, audit, failed equipment), what occurred during the event, why the event occurred (if known), and how the event occurred (if known);

g. licensee response and corrective actions taken;

h. offsite assistance (e.g., requested or not requested, arrived, status);

i. media interest, if any, including licensee issued press releases; and

j. source(s) of information (e.g., licensee CST, U.S. Computer Emergency Readiness Team, law enforcement).

A follow-up written report should be provided to the NRC in accordance with the event reporting requirements of the existing regulations. Additional details on the cyber security elements of the event should be included, similar to the documentation for a recorded event as discussed in Section C.11.2.

11.2 Event Tracking

A records the following events within 24 hours of their discovery and tracks them to resolution:

a. 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

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

Although these recorded events are tracked to resolution, the licensee does not need to submit a report to the NRC. The licensee maintains documentation of the recorded events on-site and the documentation is made available for NRC inspection. Examples of recorded events include: (1) the compromise of a system, component, or cyber security control 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.

Documentation for a recorded event should contain, at a minimum, the following information, as applicable:

a. date and time of the event, including chronological timeline;

b. the FCF's operating mode at time of event (e.g., shut down or operating);

c. functions directly or indirectly affected by the event (e.g., compromised, failed, or degraded);

d. support systems or equipment directly or indirectly affected (e.g., compromised, failed, or degraded);

e. VDAs affected (e.g., compromised, failed, or degraded) by the event;

f. cyber security controls involved in the event (e.g., compromised or performed as intended);

g. personnel involved or contacted (e.g., contractors, security personnel, visitors, plant staff, perpetrators or attackers, NRC personnel, responders, and other personnel);

h. method of discovery of the event, or information (e.g., routine patrol, inspection, test, maintenance, alarm annunciation, audit, communicated threat, or unusual circumstances);

i. immediate actions taken in response to the event and any compensatory measures established;

j. description of media interest and press releases;

k. indications or records of previous similar events;

l. procedural or human errors or equipment failures;

m. cause of the event or the licensee's analysis of the event (e.g., brief summary in the report and references to any ongoing or completed detailed investigations, assessments, analyses, or evaluations);

n. corrective actions taken or planned, including dates of completion; and

o. name and phone number of a licensee's point of contact.

For failures, degradations, or discovered vulnerabilities of the cyber security program, licensees should also record the following information, as applicable, in addition to items a. through o. above:

a. description of failed, degraded, or vulnerable equipment, systems or controls (e.g., manufacturer and model number, or procedure number);

b. unusual conditions that may have contributed to the failures, degradations, or discovered vulnerabilities of the equipment, systems or controls (e.g., environmental conditions, plant outage, or software update);

c. security settings/configuration of the components, systems or controls that failed, or became degraded or vulnerable; and

d. apparent cause of component, system or control failure, degradation, or vulnerability.

The licensee is permitted and encouraged to voluntarily report cyber-related events or conditions that do not meet the criteria for required reporting if it believes that the event or condition might be of safety or security significance or of generic interest or concern. Ensuring 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 retains 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 maintains 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 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. The licensee should maintain cyber security program reviews and cyber security event reports and make them available for inspection for a period of 3 years.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[1] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC staff complies with 10 CFR 70.76, "Backfitting."

Use by Applicants and Licensees

Applicants and licensees may voluntarily[2] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide 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 regulatory guide 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 regulatory guide 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 regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this regulatory guide, 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 regulatory guide 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 regulatory guide. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of this regulatory guide, requests for information under 10 CFR 70.22(d) as to whether a licensee intends to commit to use of this regulatory guide, generic communication, or promulgation of a rule requiring the use of this regulatory guide 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 regulatory guide, 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 regulatory guide are part of the licensing basis of the facility. However, unless this regulatory guide 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 regulatory guide 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 regulatory guide and (2) the specific subject matter of this regulatory guide 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

---

1 In this section, "licensees" refers to applicants for and holders of FCF licenses through 10 CFR 40.31, "Application for Specific Licenses," or 10 CFR 70.22, "Contents of Applications."

2 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.

either follow the guidance in this regulatory guide or provide an equivalent alternative process that demonstrates compliance with the 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 regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409, "Backfitting Guidelines," (Ref. 43) and NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 44).

GLOSSARY

active consequence of concern	A consequence of concern that is directly caused by a cyber attack.
adaptive process	Changing cyber security practices based on lessons learned and predictive indicators derived from previous and current activities.
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.
Category I fuel cycle facility	A fuel cycle facility authorized to possess or use a formula quantity of strategic special nuclear material.
Category II fuel cycle facility	A fuel cycle facility authorized to possess or use special nuclear material of moderate strategic significance.
Category III fuel cycle facility	A fuel cycle facility authorized to possess or use special nuclear material of low strategic significance.
common control	Cyber security controls in place for related VDAs. Note that similar VDAs with common controls may also have shared implementing procedures.
consequence of concern	Specific results of a cyber attack that a licensee protects against in accordance with 10 CFR 73.53(c).
consequence of concern – design basis threat	Specific results of a cyber attack that a Category I fuel cycle facility licensee protects against in accordance with 10 CFR 73.53(c)(1).
consequence of concern – safeguards	Specific results of a cyber attack that a Category II fuel cycle facility licensee protects against in accordance with 10 CFR 73.53(c)(2).
consequence of concern – safety and security	Specific results of a cyber attack that all fuel cycle facility licensees protects against in accordance with 10 CFR 73.53(c)(3) and (c)(4).
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) use internal and/or external components, (3) involve physical, electronic, or digital threats, (4) be directed or nondirected in nature, (5) be conducted by threat agents who have either malicious or nonmalicious 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 CSIRP. 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 detects, protects against, and responds to a cyber attack capable of causing a consequence of concern.
Cyber Security Team	A team comprising 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 processes information, communicates data, or is programmed to manipulate licensee site machinery.
fuel cycle facility	An applicant or holder of an NRC license subject to the requirements of 10 CFR 70.60 or for uranium hexafluoride conversion or deconversion licensed under 10 CFR Part 40.
grouping of vital digital assets	Similar VDAs throughout the facility that may be addressed as a group as 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 VDAs 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 VDA to address the performance specifications of the applicable cyber security controls.
inherited control	A specific cyber security measure taken for a parent VDA that is credited by a subordinate VDA to address the performance specification of a cyber security control. 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.
integrated administration	Implementing an organization-wide approach to managing the cyber security program that uses risk informed policies, processes, and procedures to address issues.
latent consequence of concern	A consequence of concern that results from a secondary event that exploits the compromise of a digital asset.
measure	A capability, item, or action (e.g., computer hardware, software, and 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, and data) necessary for a VDA to function properly. A support system may also be a device (e.g., meter, laptop, and smart phone) used for calibration and testing a VDA. A support system is protected if its compromise could (1) directly cause a consequence of concern, (2) provide an input to a VDA that causes a consequence of concern, or (3) preclude the VDA 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 VDA.
temporary compensatory measure	An interim capability, item, or action taken to address a degraded measure established to address the performance specifications of a cyber security control.
vital digital asset	A digital asset for which no alternate means has been identified to prevent the associated consequence of concern.

Note: Appendix B to NIST SP 800-53, Rev. 4, provides definitions for terms that do not appear in this glossary and are used within Appendix B, C, D, E, or F.

REFERENCES[3]

1. *U.S. Code of Federal Regulations* (CFR), "Physical Protection of Plants and Materials," Part 73, Section 53, "Requirements for cyber security at nuclear fuel cycle facilities," Title 10, "Energy."

2. CFR, "Domestic Licensing of Source Material," Part 40, Title 10, "Energy."

3. CFR, "Domestic Licensing of Source Material," Part 40, Section 40.31, "License applications," Title 10, "Energy."

4. CFR, "Domestic Licensing of Source Material," Part 40, Section 40.35(g), "Conditions of specific licenses issued pursuant to 10 CFR 40.34," Title 10, "Energy."

5. CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Title 10, "Energy."

6. CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Section 70.22, "Contents of application," Title 10, "Energy."

7. CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Section 70.32(f), "Conditions of licenses," Title 10, "Energy."

8. CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Section 70.61, "Performance requirements," Title 10, "Energy."

9. CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Section 70.62, "Safety program and integrated safety analysis," Title 10, "Energy."

10. CFR, "Physical Protection of Plants and Materials," Part 73, Title 10, "Energy."

11. CFR, "Physical Protection of Plants and Materials," Part 73, Section 73.1(a)(1), "Radiological sabotage," Title 10, "Energy."

12. CFR, "Physical Protection of Plants and Materials," Part 73, Section 73.1(a)(2), "Theft or diversion of formula quantities of strategic special nuclear material," Title 10, "Energy."

13. CFR, "Physical Protection of Plants and Materials," Part 73, Section 73.20, "General performance objective and requirements," Title 10, "Energy."

14. CFR, "Physical Protection of Plants and Materials," Part 73, Section 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance," Title 10, "Energy."

15. CFR, "Physical Protection of Plants and Materials," Part 73, Section 73.46(g)(6), "Fixed site physical protection systems, subsystems, components, and procedures," Title 10, "Energy."

---

[3] 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.

16. CFR, "Physical Protection of Plants and Materials," Part 73, Section 73.54, "Protection of digital computer and communication systems and networks," Title 10, "Energy."

17. CFR, "Material Control and Accounting of Special Nuclear Material," Part 74, Title 10, "Energy."

18. CFR, "Material Control and Accounting of Special Nuclear Material," Part 74, Section 74.41, "Nuclear material control and accounting for special nuclear material of moderate strategic significance," Title 10, "Energy."

19. CFR, "Material Control and Accounting of Special Nuclear Material," Part 74, Section 74.51, "Nuclear material control and accounting for strategic special nuclear material," Title 10, "Energy."

20. CFR, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," Part 95, Title 10, "Energy."

21. U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide 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," Washington, DC. (Non-Public)[4]

22. NRC, "Issuance of Order for Interim Compensatory Measures – Global Nuclear Fuel – Americas, LLC Wilmington, NC" Washington, DC, February 06, 2003. (ADAMS Accession No. ML022480420)

23. NRC, "Issuance of Order for Interim Compensatory Measures – Framatome Advanced Nuclear Power, Inc. Richland, WA" Washington, DC, February 06, 2003. (ADAMS Accession No. ML022480387)

24. NRC, "Issuance of Order for Interim Compensatory Measures – Westinghouse Electric Company LLC Columbia, SC" Washington, DC, February 06, 2003. (ADAMS Accession No. ML022480445)

25. NRC, "Issuance of Order for Interim Compensatory Measures – Nuclear Fuel Services, Inc. Irwin, TN" Washington, DC, February 06, 2003. (ADAMS Accession No. ML031910753)

26. NRC, "Issuance of Order for Interim Compensatory Measures – BWX Technologies Lynchburg, VA" Washington, DC, April 29, 2003. (ADAMS Accession No. ML15314A256)

27. NRC, "Issuance of Order for Interim Compensatory Measures – Honeywell International, Inc. Metropolis, IL" Washington, DC, August 18, 2004. (ADAMS Accession No. ML042240002)

28. NRC, "Design Basis Threat," *Federal Register*, Vol. 72, No. 52: pp. 12705 (72 FR 12705), Washington, DC, March 19, 2007.

29. NRC, "Power Reactor Security Requirements" *Federal Register*, Vol. 74, No. 58: pp. 13926, (74 FR 13926), Washington, DC, March 27, 2009.

[4] This document is not publicly available because it contains classified information.

30. NRC, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

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

32. NRC, SECY-14-0147, "Cyber Security for Fuel Cycle Facilities," Washington, DC, December 30, 2014. (ADAMS Accession No. ML14177A264)[5]

33. NRC, Staff Requirements Memorandum to SECY-14-0147, "Staff Requirements – SECY-14-0147 – Cyber Security for Fuel Cycle Facilities," Washington, DC, March 24, 2015. (ADAMS Accession No. ML15083A175)

34. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, Gaithersburg, MD, April 2013.[6]

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

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

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

38. International Atomic Energy Agency (IAEA) Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," Vienna, Austria, 2011.[7]

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

40. 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.

41. 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.[8]

---

5 This document is not publicly available because it contains sensitive, security-related information.

6 Copies of NIST computer-security documents may be obtained through its Web site at 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.

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

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

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

43. NRC, "Backfitting Guidelines," NUREG-1409, Revision 2, Washington, DC, July 1990. (ADAMS Accession No. ML032230247)

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

[9] Copies of documents may be obtained from Standardization, ISO Central Secretariat, BIBC II, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland.

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]

CHAPTER 1 CONTENTS OF THE CYBER SECURITY PLAN

This cyber security plan (CSP or the Plan) is submitted by [FULL NAME] (hereafter called [NAME]) to the U.S. Nuclear Regulatory Commission (NRC) to satisfy the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53, "Requirements for Cyber Security at Nuclear Fuel Cycle Facilities." 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 are to be withheld from public disclosure in accordance with the provisions of 10 CFR 2.790(d) because 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. Chapters 2 through 10 of the Plan discuss details of this program. Additional descriptions of the process and special authorizations are given in the [LICENSING DOCUMENTATION].

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

2.1 INTRODUCTION

This CSP contains commitments for [NAME] to establish, implement, and maintain a cyber security program 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 toward vital digital assets (VDAs). The detection functions include multiple data collection points, in-depth analysis mechanisms, and appropriate threat intelligence. Protection is accomplished by either: (1) taking measures for VDAs to address the performance specifications of cyber security controls that have been established to protect against a specific consequence of concern; or (2) monitoring and maintaining alternate means to perform the functions of digital assets whose compromise by a cyber attack could result in a consequence of concern. To remain effective, this protection is monitored and maintained. In addition, [NAME] implements compensatory measures to protect VDAs in the event cyber security controls fail, become degraded, or are not operating as intended. [NAME] maintains the capability to respond to a cyber attack capable of causing a consequence of concern. A cyber security incident response plan (CSIRP) [PROVIDE REFERENCE TO SEPARATE DOCUMENT OR APPLICABLE SECTION OF THIS PLAN] is maintained on-site to identify the specific steps and actions to respond to a cyber attack that could result in a consequence of concern. The CSIRP describes the structure and organization of the cyber security incident response (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 DETECTS A CYBER ATTACK CAPABLE OF CAUSING A CONSEQUENCE OF CONCERN.]

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

[PROVIDE AN OVERVIEW OF HOW THE PROGRAM RESPONDS 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. A cyber security program is developed and maintained that detects, protects against, and responds to a cyber attack capable of causing a consequence of concern as identified in 10 CFR 73.53(c).
b. A Cyber Security Team (CST) is 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).
c. For VDAs, cyber security controls are 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).
d. For VDAs, written implementing procedures are 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)
e. The cyber security program includes appropriate temporary compensatory measures, configuration management, documentation, recordkeeping, and reporting to the NRC.
f. Identification and documentation of digital assets and VDAs is completed within 6 months of NRC approval of this Plan.
g. Full implementation of this Plan occurs within 18 months of its approval by NRC.

CHAPTER 3 CYBER SECURITY TEAM

[DESCRIBE THE STRUCTURE AND FUNCTIONS 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 ON-SITE DOCUMENTATION OF THE NAMES AND CONTACT INFORMATION FOR INDIVIDUALS FILLING KEY POSITIONS ON THE TEAM RATHER THAN INCORPORATING THEM IN THE PLAN.]

3.2 DUTIES AND RESPONSIBILITIES

[DEFINE THE POSITION ROLES AND RESPONSIBILITIES. DEFINE SPECIFIC DUTIES AND FUNCTIONS FOR THE CYBER SECURITY TEAM AS A WHOLE. DESCRIBE THE VDA AUTHORIZATION PROCESS FOR THE FULLY IMPLEMENTED CYBER SECURITY PROGRAM.]

3.3 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.]

3.4 EQUIPMENT

[DOCUMENT A COMMITMENT TO PROVIDE THE CST WITH THE APPROPRIATE SOFTWARE, TOOLS, AND DEVICES TO VERIFY THAT 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 IS MANAGED. PROVIDE THE GOALS FOR OPERATION AFTER THE PROGRAM IS FULLY IMPLEMENTED. DESCRIBE HOW THE CST AND ITS FUNCTIONS PROVIDE SUPPORT OF THE CYBER SECURITY PROGRAM FOR THE LIFE OF THE FACILITY.]

[DESCRIBE HOW MANAGEMENT PRACTICES ARE 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 CSIRP INTO THE CSP OR PROVIDE THE INFORMATION BY REFERENCE TO A SEPARATE CSIRP. IF A SEPARATE DOCUMENT IS USED, PROVIDE A SUFFICIENT COMMITMENT IN THE CSP TO MAKE THE CSIRP ENFORCEABLE.]

[DESCRIBE THE CYBER ATTACK DETECTION ACTIVITIES USED.]

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

[DESCRIBE THE STRUCTURE OF THE CSIR TEAM AND HOW IT IS ALLOCATED RECOURSES NECESSARY FOR RESPONSE AND HOW STAFF IS 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 OF SUCH TESTING.]

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:

a. radiological sabotage, as specified in 10 CFR 73.1(a)(1);
b. theft or diversion of formula quantities of strategic special nuclear material, as specified in 10 CFR 73.1(a)(2); or
c. 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:

a. unauthorized removal of special nuclear material of moderate strategic significance, as specified in 10 CFR 73.67(d), or
b. 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:

a. radiological exposure of 0.25 Sv (25 rem) or greater for any individual,
b. 30 milligrams or greater intake of uranium in soluble form for any individual outside the controlled area, or
c. 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 one or more of the following:

a. radiological exposure of 0.25 Sv (25 rem) or greater for any individual,
b. 30 milligrams or greater intake of uranium in soluble form for any individual outside the controlled area,
c. an acute chemical exposure that could lead to irreversible or other serious long-lasting health effects for any individual, or
d. 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 IS 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, AND 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 THE NRC TO DETERMINE THE APPROACH.]

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

A. THE NAME AND PHYSICAL LOCATION OF THE APPLICATION, DEVICE, SYSTEM, OR NETWORK IDENTIFIED AS A DIGITAL ASSET, AND

B. THE TYPES OF CONSEQUENCES OF CONCERN THAT 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. A GENERAL DESCRIPTION, INCLUDING THE PHYSICAL AND LOGICAL LOCATION, OF EACH APPLICATION, DEVICE, SYSTEM, OR NETWORK IDENTIFIED AS A VDA;

B. 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

C. 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, IF COMPROMISED, COULD 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 THAT THE LICENSEE USES TO GROUP SIMILAR VDAs, WHEN APPROPRIATE.]

[WHEN A GROUPING OF VDAs IS USED, PROVIDE A COMMITMENT TO DOCUMENT THE JUSTIFICATION FOR THIS GROUPING 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, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY STANDARDS, AND INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 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 ARE 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 ARE USED, DESCRIBE HOW THEY ARE IMPLEMENTED.]

7.5 VERIFYING CYBER SECURITY CONTROLS

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

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

CHAPTER 8 IMPLEMENTING PROCEDURES AND TEMPORARY COMPENSATORY MEASURES

8.1 IMPLEMENTING PROCEDURES

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

Implementing procedures identify and document the cyber security controls applicable to VDAs. An implementing procedure:

a. provides a network diagram reference and physical location for the VDA;
b. identifies the VDA and its boundary;
c. lists the associated type of consequence of concern;
d. provides the function, general description, and purpose of the VDA;
e. lists the individual(s) or organization responsible for the VDA;
f. describes the location, interconnections, and operating environment of the VDA;
g. documents applicable support systems;
h. identifies tools used in the operation, calibration, or maintenance of the VDA;
i. lists an inventory of the VDA components (e.g., hardware, peripherals, firmware, and software) necessary to support configuration management;
j. documents the measures taken to meet the performance specifications associated with the identified cyber security controls; and
k. describes the verification process for cyber security controls.

8.2 TEMPORARY COMPENSATORY MEASURES

[PROVIDE A COMMITMENT TO USE TEMPORARY COMPENSATORY MEASURES WHEN AND WHERE NECESSARY.]

[PROVIDE A COMMITMENT TO DOCUMENT THE FUNCTION OF A TEMPORARY COMPENSATORY MEASURE, HOW IT EFFECTIVELY ADDRESSES THE PERFORMANCE SPECIFICATION OF THE CYBER SECURITY CONTROL, AND THE TIMETABLE ASSOCIATED WITH ITS UTILIZATION]

[DESCRIBE HOW THE TEMPORARY COMPENSATORY MEASURES 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 ARE COMPLETED.]

9.2 SITE-WIDE CONSIDERATIONS

[DESCRIBE THE INTEGRATION OF THE CYBER SECURITY PROGRAM PERFORMANCE OBJECTIVES INTO THE SITE-WIDE CONFIGURATION MANAGEMENT SYSTEM.]

CHAPTER 10 REVIEW OF THE CYBER SECURITY PROGRAM

A review of the cyber security program occurs as follows:

a. [CATEGORY I FACILITIES ONLY – as a component of the security program in accordance with the requirements of 10 CFR 73.46(g)(6).]
b. [ALL OTHER FACILITIES – at least every 36 months.]

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

a. purpose, scope, roles, responsibilities, requirements, and management commitments of the cyber security program;
b. changes made to implementing procedures;
c. measures of performance established through cyber security controls and whether the licensee developed, monitored, and reported on the results these measures of performance;
d. cyber security control strategy;
e. use of alternate means and defensive architecture for digital assets;
f. facility's CSIR capability;
g. configuration management system; and
h. changes made to the operating environment.

The findings, deficiencies, and recommendations resulting from the review are:

a. tracked and addressed in a timely manner, and
b. documented in a report to the [INSERT POSITION 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 is 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 are recorded within 24 hours of discovery and tracked to resolution:

a. a failure, compromise, discovered vulnerability, or degradation that results in a decrease in effectiveness of a cyber security control protecting a VDA;

[FOR CATEGORY I FACILITIES ONLY –

b. a cyber attack that compromises a VDA associated with the loss of nuclear material control and accounting for strategic special nuclear material, as specified in 10 CFR 74.51(a)]; and

[FOR CATEGORY II FACILITIES ONLY –

c. 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] are used to record 24-hour cyber security events.

CHAPTER 12 RECORDKEEPING

The licensee retains supporting technical documentation that demonstrates compliance with the requirements of 10 CFR 73.53 as a record. All records, reports, and documents required to be kept by Commission regulations, orders, or license conditions are maintained and made available for inspection until the NRC terminates the license. The licensee maintains superseded portions of these records, reports, and documents 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 the National Institute for Standards and Technology (NIST) report entitled, "Framework for Improving Critical Infrastructure Cyber Security," Version 1, issued February 2014)

[Licensee/Applicant] does the following:

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

B-2 Policies and Procedures

(Informed by NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, issued April 2013)

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

a. access control,
b. security awareness and training,
c. audit and accountability,
d. system and information integrity,
e. identification and authentication,
f. system maintenance,
g. media protection,
h. system and services acquisition, and
i. system and communications protection.

These policies and procedures do the following:

a. Address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
b. Facilitate the implementation of the policy and associated security controls.

[Licensee/Applicant] reviews and updates the policies and procedures at least every 24 months when changes occur in VDAs, the environment that may adversely impact the cyber security program, or its ability to prevent a consequence of concern.

B-3 Separation of Duties
(Informed by NIST SP 800-53, Revision 4, AC-5)

[Licensee/Applicant] does the following:

a. Separate the duties of VDA management, programming, configuration management, quality assurance and testing, and network security for VDAs.
b. Document the separation of duties of individuals.
c. Define access authorizations to support separation of duties.

B-4 Least Privilege
(Informed by NIST SP 800-53, Revision 4, AC-6)

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

B-5 Authorize Access to Security Functions
(Informed by NIST SP 800-53, Revision 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 Nonprivileged Access for Nonsecurity Functions
(Informed by NIST SP 800-53, Revision 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 nonprivileged accounts or roles when accessing nonsecurity functions.

B-7 Network Access to Privileged Commands
(Informed by NIST SP 800-53, Revision 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, Revision 4, AC-6 (5))

[Licensee/Applicant] restricts privileged accounts on the VDA to personnel or roles that, due to the design of the VDA, are required to 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, Revision 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 that do not require identification or authentication.

B-10 Privileged Commands and Access
(Informed by NIST SP 800-53, Revision 4, AC-17 (4))

[Licensee/Applicant] does the following:

a. Authorize the execution of privileged commands and access to security-relevant information via remote access only for the necessary, safe operation of the VDA or prevention of a consequence of concern.
b. Document 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, Revision 4, AC-19)

[Licensee/Applicant] does the following:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for mobile devices.
b. Authorize the connection of mobile devices to organizational VDAs.

B-12 Full-Device or Container-Based Encryption
(Informed by NIST SP 800-53, Revision 4, AC-19 (5))

[Licensee/Applicant] uses 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, Revision 4, AC-22)

[Licensee/Applicant] does the following:

a. Designate individuals authorized to post information to a publicly accessible VDA.
b. Train authorized individuals to ensure that publicly accessible information does not contain security sensitive information.
c. Review the proposed content of information before posting to the publicly accessible VDA to ensure that nonpublic information is not included.
d. Review the content of the publicly accessible VDA for nonpublic information at least every 30 days and remove such information, if it is discovered.

B-14 LOG Events
(Informed by NIST SP 800-53, Revision 4, AU-2)

[Licensee/Applicant] does the following:

a. Develop and document a list of auditable records that provide adequate information to prevent a consequence of concern, including, at a minimum, the following events:
   (1) user login or logouts;
   (2) configuration, software, or firmware changes;
   (3) audit setting changes;
   (4) privileged access or commands; and
   (5) any modifications of the security functions of VDAs.
b. Determine that the VDA is capable of generating auditable records that can be reviewed in a timely manner.
c. Coordinate 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.

d. Provide 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, Revision 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, Revision 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 record retention requirements.

B-17 VDA Connections
(Informed by NIST SP 800-53, Revision 4, CA-3**)**

[Licensee/Applicant] does the following:
a. Authorize connections from the VDA to other digital assets.
b. For each interconnection, document the interface characteristics, security requirements, and the nature of the information communicated.
c. Review and update the authorizations at least every 12 months.

B-18 Continuous Monitoring
(Informed by NIST SP 800-53, Revision 4, CA-7)

[Licensee/Applicant] develops a continuous monitoring strategy and implements a continuous monitoring program that includes the following tasks:
a. establishment and monitoring of sufficient cyber security metrics to provide adequate confirmation that security controls are in place and effective;
b. establishment, justification, and documentation of the monitoring and assessment frequencies for each metric;
c. ongoing security control assessments in accordance with the continuous monitoring strategy;
d. ongoing security status monitoring of cyber security metrics in accordance with the continuous monitoring strategy;
e. correlation and analysis of security-related information generated by assessments and monitoring;
f. response actions to address results of the analysis of security-related information; and
g. documentation of the security status of the VDAs and their operating environment by the Cyber Security Team at least every 30 days.

B-19 Baseline Configuration
(Informed by NIST SP 800-53, Revision 4, CM-2 and CM-2 (1))

[Licensee/Applicant] does the following:
a. Develop, document, and maintain under configuration control a current baseline configuration of the VDA.
b. Review the baseline configuration of the VDA when required because of an identified vulnerability, relevant change in threat intelligence, or suspected compromise.

c. Update 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, Revision 4, CM-3 (1))

[Licensee/Applicant] uses automated mechanisms to do the following:
a. Document proposed changes to the VDA.
b. Notify appropriate personnel of proposed changes to the VDA and request change approval.
c. Prohibit changes to the VDA until receipt of designated approvals.
d. Document all changes to the VDA.
e. Notify appropriate personnel when approved changes to the VDA are completed.

B-21 Access Control for Transmission Medium
(Informed by NIST SP 800-53, Revision 4, PE-4)

[Licensee/Applicant] controls physical access to VDA distribution and transmission lines to adequately protect them to prevent a consequence of concern.

B-22 Access Control for Output Devices
(Informed by NIST SP 800-53, Revision 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, Revision 4, PL-2 and PL-2 (3))

[Licensee/Applicant] does the following:
a. Develop implementing procedures for each VDA that do the following:
   (1) Provide the associated consequence of concern for the VDA, including supporting rationale.
   (2) Describe the operational environment for the VDA and relationships with or connections to other digital assets.
   (3) Provide an overview of the security requirements for the VDA.
   (4) Describe the cyber security measures in place or planned for meeting cyber security control requirements, including a rationale for equivalent measures.
b. Distribute copies of the implementing procedures and communicate subsequent changes to the procedures only to authorized personnel with a need to know.
c. Update 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.
d. Protect the implementing procedures from unauthorized disclosure and modification.
e. Plan and coordinate security-related activities affecting the VDA with the Cyber Security Team before conducting such activities to reduce the impact on other organizational entities.

B-24 Cyber Security Architecture
(Informed by NIST SP 800-53, Revision 4, PL-8 and PL-8 (1))

[Licensee/Applicant] does the following:
a. Document a cyber security architecture for the VDA that does the following:

(1) describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of VDA or related information, and

(2) describes any security assumptions about and dependencies on external services.

b. Review and update the cyber security architecture at least every 24 months to reflect updates.

c. Ensure 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 does the following:

a. uses complementary and redundant cyber security measures that establish multiple layers of protection to safeguard VDAs,

b. ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner, and

c. ensures the capability to detect, prevent, respond to, and mitigate cyber attacks.

B-25 Acquisition Process

(Informed by NIST SP 800-53, Revision 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:

a. security functional requirements,

b. security strength requirements,

c. security assurance requirements,

d. security-related documentation requirements,

e. requirements for protecting security-related documentation,

f. a description of the VDA development environment and environment in which the VDA is intended to operate, and

g. acceptance criteria.

B-26 Functional Properties of Security Controls

(Informed by NIST SP 800-53, Revision 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 do the following:

a. Describe the functional security properties, design, and implementation information to be used with sufficient documentation to support the licensee's conclusions that the functional security features work as intended.

b. Identify the functions, ports, protocols, and services used.

B-27 National Information Assurance Partnership – Approved Protection Profiles

(Informed by NIST SP 800-53, Revision 4, SA-4 (7))

[Licensee/Applicant] does the following:

a. Limit the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance Partnership (NIAP)-approved protection profile for a specific technology type, if such a profile exists.

b. Require the NIST Cryptographic Module Validation Program to validate the cryptographic module 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.

B-28 Use of Approved PIV Products
(Informed by NIST SP 800-53, Revision 4, SA-4 (10))

[Licensee/Applicant] uses only technology on the list of approved products under Federal Information Processing Standard Publication 201-2, "Personal Identity Verification of Federal Employees and Contractors," dated August 2013, for personal identity verification capabilities used to protect VDAs.

B-29 VDA Documentation
(Informed by NIST SP 800-53, Revision 4, SA-5)

[Licensee/Applicant] does the following:

a. Obtain administrator documentation for the VDA, component, or service that describes the following:
   (1) secure configuration, installation, and operation;
   (2) effective use and maintenance of security functions and mechanisms; and
   (3) known vulnerabilities of the configuration and use of administrative and privileged functions.
b. Obtain user documentation for the VDA, component, or service that describes the following:
   (1) user-accessible security functions and mechanisms and how to effectively use those security functions and mechanisms;
   (2) methods for user interactions that enable individuals to use the VDA, component, or service in a more secure manner; and
   (3) user responsibilities in maintaining the security of the VDA, component, or service.
c. Document 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.
d. Protect documentation from unauthorized access.
e. Distribute documentation to authorized personnel on a need-to-know basis.

B-30 Security Engineering Principles
(Informed by NIST SP 800-53, Revision 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, Revision 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, Revision 4, SC-18)

[Licensee/Applicant] does the following:

a. Define a technical basis for acceptable and unacceptable mobile code and mobile code technologies to prevent a consequence of concern.
b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
c. Authorize, monitor, and control the use of mobile code within the VDA.

B-33 Information Input Validation

(Informed by NIST SP 800-53, Revision 4, SI-10)

[Licensee/Applicant] does the following:

a. Ensure that the VDA checks the validity of information inputs automatically for accuracy, completeness, validity, and authenticity.
b. Enforce the documentation of rules for checking the valid syntax of VDA inputs (e.g., character set, length, numerical range, and acceptable values) and ensure that the rules are in place to verify that inputs match specified definitions for format and content.
c. Confirm 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, Revision 4, CM-1)

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

a. addresses roles, responsibilities, and configuration management processes and procedures;
b. establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. defines the configuration items for the VDA and places the configuration items under configuration management; and
d. protects the configuration management plan from unauthorized disclosure and modification.

B-35 Security Awareness Training

(Informed by NIST SP 800-53, Revision 4, AT-1)

[Licensee/Applicant] does the following:

a. Provide basic security awareness training to VDA users (including managers, senior executives, and contractors) as follows:
   (1) as part of initial training for new users,
   (2) when required by VDA changes, and
   (3) at least every 12 months thereafter.
b. Provide role-based security training to personnel with assigned security roles and responsibilities as follows:
   (1) before authorizing access to the VDA or performing assigned duties,
   (2) when required by VDA changes, and
   (3) at least every 12 months thereafter.
c. Document and monitor individual VDA security training activities, including basic security awareness training and specific VDA security training.
d. Retain individual training records consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53(i).

B-36 Prohibit Nonprivileged Users from Executing Privileged Function
(Informed by NIST SP 800-53, Revision 4, AC-6 (10))

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

B-37 Unsuccessful Logon Attempts
(Informed by NIST SP 800-53, Revision 4, AC-7)

[Licensee/Applicant] does the following:

a. Limit 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 automatically locks out the account).
b. Ensure that the VDA enforces the lockout mode automatically.

B-38 Purge or Wipe Mobile Device
(Informed by NIST SP 800-53, Revision 4, AC-7 (2))

[Licensee/Applicant] ensures that mobile devices used with VDAs purge or wipe 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, Revision 4, AC-8)

[Licensee/Applicant] ensures that VDAs display to users a use notification message or banner before granting access that provides appropriate security notices consistent with U.S. Nuclear Regulatory Commission regulations and supports the prevention of a consequence of concern. The VDAs retain 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 of the following:

a. Users are accessing a VDA.
b. Usage may be monitored, recorded, and subject to audit.
c. Unauthorized use is prohibited and subject to criminal and civil penalties.
d. Use indicates consent to monitoring and recording.
e. For publicly accessible VDAs, the notice does the following:
    (1) displays VDA use information before granting further access;
    (2) displays references, if any, to monitoring, recording, or auditing that are consistent with the requirements for nonpublic VDAs; and
    (3) includes a description of the authorized uses.

B-40 Concurrent Session Control
(Informed by NIST SP 800-53, Revision 4, AC-10)

[Licensee/Applicant] ensures that 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, Revision 4, AC-11 and AC-12)

[Licensee/Applicant] ensures that the VDA does the following:

a. 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;
b. retains the session lock until the user reestablishes access using established identification and authentication procedures; and
c. automatically terminates a user session within 45 minutes of inactivity.

B-42 Automated Monitoring/Control
(Informed by NIST SP 800-53, Revision 4, AC-17 (1))

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

B-43 Protection of Confidentiality/Integrity Using Encryption
(Informed by NIST SP 800-53, Revision 4, AC-17 (2))

[Licensee/Applicant] ensures that 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, Revision 4, AC-18 (1))

[Licensee/Applicant] ensures that 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, Revision 4, AU-7)

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

a. supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents and
b. does not alter the original content or time ordering of audit records.

B-46 Automatic Processing
(Informed by NIST SP 800-53, Revision 4, AU-7 (1))

[Licensee/Applicant] ensures that 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, Revision 4, AU-8)

[Licensee/Applicant] does the following:

a. Use a time source that is protected at an equal or greater level than the VDAs it supports.
b. Ensure that the VDA does the following:
   (1) implements time synchronization mechanisms that do not introduce a vulnerability leading to a consequence of concern,
   (2) synchronizes its internal clock from the protected time source, and

(3) uses its internal clock to generate time stamps for audit records.

B-48 Supply Chain Protection
(Informed by NIST SP 800-53, Revision 4, SA-12)

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

a. establishing trusted distribution paths,
b. validating vendors, and
c. 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, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, issued April 2013, 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, Revision 4, AC-2)

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

a. Assign account managers for VDA accounts.
b. Establish conditions for group and role membership.
c. Specify authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
d. Require independent management approval for requests to create VDA accounts.
e. Create, enable, modify, disable, and remove VDA accounts in accordance with the access control policy.
f. Monitor the use of VDA accounts.
g. Notify account managers in a timely manner of the following:
    (1) when accounts are no longer required,
    (2) when users are terminated or transferred, and
    (3) when individual VDA usage or need to know changes.
h. Authorize access to the VDA based on the following:
    (1) a valid access authorization and
    (2) intended VDA usage.
i. Review accounts at least every 30 days for compliance with account management requirements.
j. Take, at a minimum, the following measures to restrict the creation and issuance of shared/group VDA accounts:
    (1) Ensure that shared/group account requests are issued only when necessary to prevent a consequence of concern, include a documented technical justification, and are reviewed and approved by the Cyber Security Team (CST) before issuance.
    (2) Automatically terminate and establish 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, Revision 4, AC-2(5), AC-2(12), and AC-2(13))

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

a. Require that users log out within 15 minutes of inactivity unless the login session is required to be maintained to prevent a consequence of concern.
b. Monitor VDA accounts for atypical usage and anomalous activity that could indicate account compromise.
c. Report atypical usage of VDA accounts to the CST.
d. Disable user accounts that have been potentially compromised upon discovery.

C-4 Automated Account Management
(Informed by NIST SP 800-53, Revision 4, AC-2 (1), AC-2 (2), AC-2 (3), AC-2 (4), and AC-2 (11))

To support the management of VDA accounts, [Licensee/Applicant] uses, at minimum, automated technical mechanisms that do the following:

a. Automatically remove or disable temporary and emergency accounts once they are no longer needed.
b. Automatically disable inactive accounts within 30 days.
c. Automatically audit account creation, modification, enabling, disabling, and removal actions and notify appropriate personnel in a timely manner.

C-5 Access Management
(Informed by NIST SP 800-53, Revision 4, AC-3, AC-3 (2), AC-4, AC-4 (4), and AC-4 (21))

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

a. logical access to VDA information and VDA resources in accordance with applicable access control policies and
b. control of the flow of information within the VDA and between interconnected systems and VDAs.

[Licensee/Applicant] ensures that the VDA uses automated technical measures that do the following:

a. Enforce dual authorization for privileged commands, operations, or access.
b. Prevent encrypted information from bypassing content-checking mechanisms.
c. Separate information flows logically or physically.
d. Notify the user, upon successful logon/access, of the following:
    (1) the date and time of the last logon/access,
    (2) the number of unsuccessful logon/access attempts since the last successful logon/access,
    (3) the number of successful and unsuccessful logons/accesses within the last 7 days, and
    (4) 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, Revision 4, AC-16, AC-16 (4), SC-16, and SC-16 (1))

[Licensee/Applicant] does the following:

a. Provide the means to associate security attributes with information in storage, in process, and/or in transmission.
b. Ensure that the security attribute associations are made and retained with the information.
c. Establish the permitted security attributes for VDAs.
d. Determine the permitted values or ranges for each of the established security attributes.
e. Support the association of security attributes for the VDA with information exchanged or transmitted between digital assets, VDAs, and components.
f. Validate the integrity of transmitted security attributes for the VDA.

C-7 Managed Access Control Points
(Informed by NIST SP 800-53, Revision 4, AC-17 (3))

[Licensee/Applicant] prohibits all remote and offsite access to VDAs. Access to VDAs is from a digital asset that is in a protected status equivalent to the VDA.

C-8 Use of External Information Systems
(Informed by NIST SP 800-53, Revision 4, AC-20 (3), and AC-20 (4))

[Licensee/Applicant] does the following:

a. Prohibit the use of nonlicensee-owned information systems, VDA components, or devices used with VDAs.
b. Prohibit the use of organization-controlled network accessible storage devices in external information systems.

C-9 Cyber Security Training
(Informed by NIST SP 800-53, Revision 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, Revision 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 that the VDA does the following:

a. 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
b. generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum, the following:
   (1) account (user or service) login failure and success;
   (2) account role or privilege change;
   (3) file or object creation, modification, and deletion;

(4) service start and stop;
(5) privileged service call;
(6) account creation, modification, and deletion;
(7) account rights assignment and removal;
(8) audit policy change;
(9) user account password change;
(10) user group creation, modification, and deletion; and
(11) remote session start, stop, and failure.

[Licensee/Applicant] ensures that the VDA auditing function does the following:

a. alerts cyber security personnel in near real time of an audit processing failure or the occurrence of an audit failure event that could indicate VDA compromise,
b. takes automated measures to preserve audit data,
c. provides the capability to increase or modify audit record content in response to threat intelligence,
d. initiates session audits at VDA startup,
e. provides the capability for authorized users to select a user session to capture/record or view/hear,
f. provides the capability for authorized users to capture/record and log content related to a user session, and
g. 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, Revision 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] does the following:

a. Allocate sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configure auditing to prevent exceedance of the storage capacity.
b. Authorize access to management of audit functionality on to authorized users with cyber security responsibilities.
c. Enforce dual authorization for movement or deletion of audit information.
d. Specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit information.
e. Ensure that the VDA provides an alert to authorized personnel when the allocated audit record storage volume reaches 80 percent of the repository maximum audit record storage capacity.
f. Ensure that the VDA backs up audit records onto a physically different VDA from the VDA being audited.
g. Ensure that the VDA protects audit information and audit tools from unauthorized access, modification, and deletion.
h. Ensure that the VDA implements cryptographic mechanisms to protect the integrity of audit information and audit tools.
i. Ensure that 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, Revision 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] does the following:

a. Use automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
b. Review and analyze VDA audit records in a timely manner for indications of potential compromise.
c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
d. Integrate 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.
e. Correlate information from audit records with information obtained from monitoring physical access to the VDA to further enhance the ability to identify potential unauthorized activity.
f. Report findings to the CST.
g. Ensure that 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 that the VDA does the following:

a. maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released,
b. validates the binding of the information reviewer identity to the information at the transfer or release points before release/transfer, and
c. 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, Revision 4, CA-2)

[Licensee/Applicant] does the following:

a. Develop a security assessment plan that describes the scope of the assessment and includes the following:
   (1) security controls and control enhancements under assessment,
   (2) assessment procedures to be used to determine security control effectiveness, and
   (3) assessment environment, assessment team, and assessment roles and responsibilities.
b. Assess 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.
c. Produce a security assessment report that documents the results of the assessment.
d. Include and document the following as part of VDA security control assessments:
   (1) an attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
   (2) announced assessments that include the following:
      – 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
      – insider threat assessment (to be done at least every 92 days); and

(3) unannounced assessments (in addition to announced assessments above) that include the following:
- 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), and
- performance/load testing (to be done at least every 183 days).

e. Provide the results of the security control assessment to the CST.
f. Restrict 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, Revision 4, CA-2 (1), CA-7 (1), CA-8, CA-8 (1), CA-8 (2))

[Licensee/Applicant] does the following:
a. Use 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.
b. Use 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.
c. Conduct penetration testing at least every 183 days on the VDA.
d. Use red team exercises to simulate attempts by adversaries to compromise VDAs.
e. Use 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, Revision 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant] does the following:
a. Use a "deny-all, permit-by-exception" policy for allowing VDAs to connect to other digital assets.
b. Prohibit access from and the connection of a VDA to an external network.
c. Prohibit the direct connection of a VDA to a public network.
d. Authorize connections to the VDA.
e. For each connection, document the interface characteristics, security requirements, and the nature of the information communicated.

C-16 National Security System Connections
(Informed by NIST SP 800-53, Revision 4, CA-3 (1))

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

C-17 Temporary Compensatory Measures
(Informed by NIST SP 800-53, Revision 4, CA-5)

[Licensee/Applicant] does the following:

a. Document temporary 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.
b. Update the temporary compensatory measure plan at least every 30 days based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.
c. Restrict access to the temporary compensatory measure plan to authorized personnel with a need to know.

C-18 Internal System Connections
(Informed by NIST SP 800-53, Revision 4, CA-9)

[Licensee/Applicant] does the following:

a. Authorize internal connections of VDA components to the VDA.
b. For each connection, document the interface characteristics, security requirements, and the nature of the information communicated.

C-19 Automated Baseline Configuration
(Informed by NIST SP 800-53, Revision 4, CM-2 (2))

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

C-20 Configuration of VDAs for High-Risk Areas
(Informed by NIST SP 800-53, Revision 4, CM-2 (7))

Before transporting VDAs associated with a design-basis threat consequence of concern to locations that it considers risk significant, [Licensee/Applicant] does the following:

a. Document a detailed justification for the VDA to be transported.
b. Obtain written approval from the CST and management.
c. Document the VDA configuration baseline and component inventory before leaving controlled areas.
d. Ensure that Safeguards Information or security-related information on the VDA is purged or protected in a manner that prevents an adversary from recovering the data before leaving controlled areas.
e. Observe chain of custody of the VDA or VDA component.
f. Perform a review of the VDA configuration baseline and component inventory upon return.
g. Perform testing of the VDA to ensure that no cyber compromise has occurred.
h. Perform a security control assessment to ensure that all controls are in place, are operational, and are performing their intended functions.

C-21 Configuration Change Control
(Informed by NIST SP 800-53, Revision 4, CM-3)

[Licensee/Applicant] does the following:

a. Document changes to the VDA and provide configuration control in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53, "Requirements for Cyber Security at Nuclear Fuel Cycle Facilities."
b. Review proposed configuration-controlled changes to the VDA and approve or disapprove such changes with explicit consideration for security impact analyses before implementing them.
c. Document configuration change decisions associated with the VDA.
d. Implement approved configuration-controlled changes to the VDA.
e. Retain records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements.
f. Audit and review activities associated with configuration-controlled changes to the VDA.
g. Coordinate and provide oversight for configuration change control activities through the change management process.

C-22 Change Testing and Analysis
(Informed by NIST SP 800-53, Revision 4, CM-3 (2), CM-4, CM-4 (1), and CM-4 (2))

[Licensee/Applicant] does the following:

a. Test, validate, and document changes to the VDA before implementing the changes on the VDA.
b. Analyze changes to the VDA to determine potential security impacts before change implementation.
c. Analyze changes to the VDA in a separate test environment before implementing them in an operational environment and look for security impacts caused by flaws, weaknesses, incompatibility, or intentional malice.
d. Check 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, Revision 4, CM-5, CM-5 (1), and CM-5 (4))

[Licensee/Applicant] does the following:

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the VDA.
b. Enforce dual authorization for implementing changes to VDAs and components.
c. Enforce VDA access restrictions and support auditing of the enforcement actions.

C-24 Review VDA Changes
(Informed by NIST SP 800-53, Revision 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, Revision 4, CM-5 (3))

[Licensee/applicant] ensures that 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, Revision 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant] does the following:

a. Establish and document configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements.
b. Implement the configuration settings.
c. Identify, document, and approve any deviations from established configuration settings.
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
e. Use automated mechanisms to centrally manage, apply, and verify VDA configuration settings.
f. Report 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, Revision 4, CM-7)

[Licensee/Applicant] does the following:

a. Configure the VDA to provide only essential capabilities to perform its function and maintain safe and secure operations.
b. Prohibit or restrict the use of unneeded functions, ports, protocols, and/or services.

C-28 Periodic Review
(Informed by NIST SP 800-53, Revision 4, CM-7 (1))

[Licensee/Applicant] does the following:

a. Review the VDA continuously to identify unnecessary and/or nonsecure functions, ports, protocols, and services.
b. Disable or restrict unneeded functions, ports, protocols, and/or services identified by the review.

C-29 Authorized Software
(Informed by NIST SP 800-53, Revision 4, CM-7 (2) CM-7 (5), CM-8 (1), CM-8 (2), and CM-8 (3))

[Licensee/Applicant] does the following:

a. Identify software programs authorized to execute on the VDA.
b. Use a "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA.
c. Review and update the list of authorized software programs at least every 92 days.
d. Use automated mechanisms for the VDA (i.e., application white listing) to prevent unauthorized program execution.
e. Develop and document an inventory of information VDA components that does the following:
   (1) accurately reflects the current VDA,

(2) includes all components within the boundary of the VDA,
(3) is at the level of granularity necessary for tracking and reporting, and
(4) includes information necessary to achieve effective information VDA component accountability.

f. Review and update the VDA component inventory at least every 92 days or as part of any changes made to a VDA.
g. Update the inventory of information VDA components as an integral part of component installations, removals, and VDA updates.
h. Use automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA.
i. Use automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components.
j. Take 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, Revision 4, CM-8, CM-8 (1), CM-8 (2), CM-8 (3), and CM-8 (4))

[Licensee/Applicant] does the following:

a. Develop and document an inventory of VDA components that does the following:
(1) accurately reflects the current VDA,
(2) includes all components within the boundary of the VDA,
(3) is at the level of granularity necessary for tracking and reporting, and
(4) includes information necessary to achieve effective VDA component accountability.
b. Review and update the VDA component inventory at least every 92 days or as part of any changes to a VDA.
c. Update the inventory of VDA components as an integral part of component installations, removals, and VDA updates.
d. Use automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA.
e. Use automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components.
f. Include in the VDA component inventory information, a means for identifying individuals responsible/accountable for administering those components.
g. Take 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, Revision 4, CM-11, CM-11 (1), and CM-11 (2))

[Licensee/Applicant] does the following:

a. Establish policies governing the installation of software on VDAs consistent with configuration management in 10 CFR 73.53(f).
b. Enforce software installation policies using automated measures where supported.
c. Monitor policy compliance using automated measures where supported.
d. Ensure appropriate personnel are alerted in near real time upon detection of the unauthorized installation of software on the VDA.
e. Prohibit user installation of software on the VDA without explicit privileged status.

C-32 Identification and Authentication

(Informed by NIST SP 800-53, Revision 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 that the VDA does the following:

a. uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and nonorganizational users (or processes acting on behalf of nonorganizational users);
b. implements multifactor authentication for network access to privileged accounts;
c. implements multifactor authentication for network access to nonprivileged accounts;
d. implements multifactor authentication for local access to privileged accounts;
e. implements multifactor authentication for local access to nonprivileged accounts;
f. implements replay-resistant authentication mechanisms for network access to privileged accounts;
g. implements replay-resistant authentication mechanisms for network access to nonprivileged accounts;
h. implements multifactor authentication for remote access to privileged and nonprivileged accounts such that a device that is separate from the system gaining access provides one of the factors and that the device meets e-authentication assurance Level 4 as described in NIST SP 800-63-2, "Electronic Authentication Guideline," issued August 2013, or later revisions;
i. accepts and electronically verifies personal identity verification credentials;
j. uniquely identifies and authenticates devices before establishing a connection to a VDA; and
k. ensures that the configuration management process handles device identification and authentication based on attestation.

C-33 Identifier Management

(Informed by NIST SP 800-53, Revision 4, IA-4, IA-4 (2), and IA-4 (7))

[Licensee/Applicant] manages VDA identifiers by doing the following:

a. receiving independent management authorization to assign an individual, group, role, or device identifier;
b. selecting an identifier that identifies an individual, group, role, or device;
c. assigning the identifier to the intended individual, group, role, or device;
d. preventing reuse of identifiers to ensure that reuse does not allow unintended or unauthorized access; and
e. disabling the identifier within 30 days of inactivity.

[Licensee/Applicant] requires the registration process for receiving an individual identifier to do the following:

a. Include supervisor authorization, and
b. Be conducted in-person before a designated registration authority.

C-34 Authenticator Management

(Informed by NIST SP 800-53, Revision 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by doing the following:

a. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. establishing initial authenticator content for authenticators defined by the organization;
c. ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revocation of authenticators;
e. changing default content of authenticators before VDA installation;
f. establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. documenting authenticator types approved for use, the frequency for changing/refreshing them, and technical justification that demonstrates that this frequency provides adequate security;
h. protecting authenticator content from unauthorized disclosure and modification;
i. requiring individuals to take, and to have devices implement, specific security safeguards to protect authenticators; and
j. changing authenticators for group/role accounts when membership to those accounts changes.

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

C-35 Password-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (1))

For password-based authentication for the VDA, [Licensee/Applicant] does the following:
a. Enforce a minimum password length, strength, and complexity that is within the capabilities of the VDA and is commensurate with the required level of security.
b. Enforce password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters.
c. Enforce a sufficient number of changed characters when new passwords are created to ensure that adversaries cannot determine the current password from previous entries.
d. Store and transmit only cryptographically protected passwords.
e. Enforce lifetime restrictions for password minimums of 1 day and provide a technical basis for maximums defined and documented by the CST that prevents unauthorized access.
f. Prohibit password reuse for 10 generations.
g. Require an immediate change to a permanent password upon the first logon when temporary passwords are used for VDA logons.
h. Store written or electronic copies of master passwords in a secure location with limited access.
i. Use automated tools to determine whether password authenticators are sufficiently strong to prevent an adversary from executing a password-guessing attack.

C-36 Public Key Infrastructure-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (2))

[Licensee/Applicant] ensures that public key infrastructure-based authentication for the VDA does the following:
a. validates certifications by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information;
b. enforces authorized access to the corresponding private key;
c. maps the authenticated identity to the account of the individual or group; and
d. implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

C-37 In-Person or Trusted Third-Party Registration
(Informed by NIST SP 800-53, Revision 4, IA-5 (3))

[Licensee/Applicant] requires the registration process for receiving authenticators to 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, Revision 4, IA-5 (11))

[Licensee/Applicant] ensures that hardware token-based authentication for the VDA uses 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, Revision 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.

C-40 Cryptographic Module Authentication
(Informed by NIST SP 800-53, Revision 4, IA-7)

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

C-41 Incident Response Training
(Informed by NIST SP 800-53, Revision 4, IR-2, IR-2 (1), and IR-2 (2))

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

a. within 92 days of assuming an incident response role or responsibility,
b. when required by VDA changes, and
c. at least every 12 months.

[Licensee/Applicant] does the following:

a. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
b. Use automated mechanisms to provide a more thorough and realistic incident response training environment.

C-42 Incident Response Testing
(Informed by NIST SP 800-53, Revision 4, IR-3 and IR-3 (2))

[Licensee/Applicant] does the following:

a. Test 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 document the results of checklists, walkthrough or tabletop exercises, and simulations (parallel/full interrupt).
b. Test the incident response capability for the VDA at least every 36 months using a comprehensive exercise.
c. Coordinate incident response testing with organizational elements responsible for related plans.

C-43 Incident Handling
(Informed by NIST SP 800-53, Revision 4, IR-4, IR-4 (1), and IR-4 (4))

[Licensee/Applicant] does the following:

a. Implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
b. Coordinate incident-handling activities with contingency planning activities.
c. Incorporate lessons learned from ongoing incident-handling activities into incident response procedures, training, and testing and implement the resulting changes accordingly.
d. Use automated mechanisms to support the incident-handling process.
e. Correlate 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, Revision 4, IR-5 and IR-5 (1))

[Licensee/Applicant] does the following:
a. Track and document VDA security incidents.
b. Use 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, Revision 4, IR-6 and IR-6 (1))

[Licensee/Applicant] does the following:
a. Require personnel to report suspected cyber security incidents to the CST upon discovery.
b. Use automated mechanisms to assist in the reporting of security incidents.

C-46 Incident Response Assistance
(Informed by NIST SP 800-53, Revision 4, IR-7 and IR-7 (1))

[Licensee/Applicant] does the following:
a. Provide 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.
b. Use automated mechanisms to increase the availability of incident response-related information and support.

C-47 Information Spillage Response
(Informed by NIST SP 800-53, Revision 4, IR-9, IR-9 (1), IR-9 (2), IR-9 (3), and IR-9 (4))

[Licensee/Applicant] does the following:
a. Respond to information spills by doing the following:
   (1) identifying the specific information involved in the information system contamination,
   (2) alerting the CST of the information spill using a method of communication not associated with the spill,
   (3) isolating the contaminated information system or VDA component,
   (4) eradicating the information from the contaminated information system or VDA component,
   (5) identifying other VDAs that may have been subsequently contaminated, and
   (6) documenting the incident.
b. Assign cleared personnel with responsibility for responding to information spills.
c. Provide information spillage response training at least every 12 months.

d. Implement procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.
e. Use 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, Revision 4, MA-2 and MA-2 (2))

[Licensee/Applicant] does the following:
a. Perform and document maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern.
b. Review records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days.
c. Approve and monitor all maintenance activities whether they are performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.
d. Require that CST approve the removal of the VDA for offsite maintenance or repairs outside the licensee's positive control.
e. Sanitize equipment to remove all information from associated media before removal for offsite maintenance or repairs outside the licensee's positive control.
f. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
g. Include in records of maintenance and repairs on VDA components, at a minimum, the date, time, identification of those performing the maintenance, description of maintenance performed, and list of VDA components removed or replaced.
h. Retain records for inspection by the NRC.
i. Use automated mechanisms to schedule, conduct, and document maintenance and repairs.
j. Produce 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, Revision 4, MA-3, MA-3 (1), MA-3 (2), and MA-3 (3))

[Licensee/Applicant] does the following:
a. Approve, control, and monitor VDA maintenance tools.
b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
c. Check 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 that contains VDA information by doing the following:
a. verifying that there is no VDA information contained on the equipment,
b. sanitizing or destroying the equipment,
c. retaining the equipment within the facility, or
d. 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, Revision 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant] does the following:

a. Approve and monitor nonlocal maintenance and diagnostic activities.
b. Document and only allow 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).
c. Use strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.
d. Maintain records for nonlocal maintenance and diagnostic activities.
e. Terminate session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant] does one of the following:

a. Document the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
b. Remove the component to be serviced from the VDA before using nonlocal maintenance or diagnostic services; sanitize the component (with regard to VDA information) before removing it from licensee facilities; and, after the service is performed, inspect and sanitize the component (with regard to potentially malicious software) before reconnecting it to the VDA.

C-51 Maintenance Personnel

(Informed by NIST SP 800-53, Revision 4, MA-5, MA-5 (1), and MA-5 (2))

[Licensee/Applicant] does the following:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
b. Ensure that unescorted personnel performing maintenance on the VDA have required access authorizations.
c. Ensure that personnel performing maintenance and diagnostic activities on a VDA that processes, stores, or transmits 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.
d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
e. Implement procedures for the use of maintenance personnel who lack appropriate security clearances that include the following requirements:
    (1) Approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified to escort and supervise maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals during the performance of maintenance and diagnostic activities on the VDA.
    (2) Before 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.
f. Develop and implement alternate security safeguards in the event that an information VDA component cannot be sanitized, removed, or disconnected from the VDA.

C-52 Timely Maintenance
(Informed by NIST SP 800-53, Revision 4, MA-6)

[Licensee/Applicant] obtains maintenance support or spare parts, or both, for VDAs that are required to remain operational to prevent a consequence of concern.

C-53 Media Access
(Informed by NIST SP 800-53, Revision 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media include any active storage device, passive storage device, or passive media that have one of the following characteristics:

a. They contain information used to manage, configure, maintain, secure, or operate the VDA.
b. They are used on the VDA for any purpose.

C-54 Media Marking
(Informed by NIST SP 800-53, Revision 4, MP-3)

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

C-55 Media Storage
(Informed by NIST SP 800-53, Revision 4, MP-4)

[Licensee/Applicant] does the following:

a. Physically control and securely store VDA media.
b. Protect 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, Revision 4, MP-5 and MP-5 (4))

[Licensee/Applicant] does the following:

a. Protect and control VDA media during transport outside of controlled areas.
b. Maintain accountability for VDA media during transport outside of controlled areas.
c. Document activities associated with the transport of VDA media.
d. Restrict the activities associated with the transport of VDA media to authorized personnel.
e. Implement 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, Revision 4, MP-6, MP-6 (1), MP-6 (2), and MP-6 (3))

[Licensee/Applicant] does the following:

a. Sanitize VDA media before disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary.
b. Review, approve, track, document, and verify media sanitization and disposal actions.
c. Use sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
d. Test sanitization equipment and procedures at least every 12 months to verify that the intended sanitization is being achieved.

e. Apply nondestructive sanitization techniques to portable storage devices before their connection to the VDA.
f. Enforce dual authorization for the sanitization of media.

C-58 Media Use
(Informed by NIST SP 800-53, Revision 4, MP-7, and MP-7 (1))

[Licensee/Applicant] does the following:
a. Prohibit the use of any media with a VDA, except specifically approved VDA media with an identifiable and verifiable owner.
b. Prohibit the use of sanitization-resistant media in any VDA.

C-59 Enhancements to Access Control for Transmission Medium
(Informed by NIST SP 800-53, Revision 4, PE-4)

[Licensee/Applicant] does the following:
a. Monitor physical access to VDA transmission and distribution lines.
b. Review the physical protection measures for VDA transmission and distribution lines for tampering or indications of attempted unauthorized access.

C-60 Monitoring Physical Access
(Informed by NIST SP 800-53, Revision 4, PE-6)

[Licensee/Applicant] does the following:
a. Monitor physical access to the facility where the VDA resides to detect and respond to physical security incidents.
b. Review physical access logs in a timely manner and upon occurrence of anomalous behavior.
c. Coordinate results of reviews and investigations with the organizational incident response capability.
d. Monitor 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, Revision 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, Revision 4, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), RA-5 (5), and RA-5 (8))

[Licensee/Applicant] does the following:
a. Scan for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA or applications, or both, are identified and reported.
b. Use vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards that require the following:
    (1) enumeration of platforms, software flaws, and improper configurations;
    (2) formatting of checklists and test procedures; and
    (3) measurement of vulnerability impact.
c. Analyze vulnerability scan reports and results from security control assessments.

d. Address vulnerabilities in a timely and technically justified manner to prevent a consequence of concern.
e. Share 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).
f. Use vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned.
g. Update the VDA vulnerabilities scanned before performing a new scan.
h. Use vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information VDA components scanned and vulnerabilities checked).
i. Determine what information about the VDA is discoverable by adversaries and take measures to address the associated potential cyber security issues.
j. Implement privileged access authorization to the VDA for vulnerability scanning activities.
k. Review historic audit logs to determine whether a vulnerability identified in the VDA has been previously exploited.

C-63 External Information System Services
(Informed by NIST SP 800-53, Revision 4, SA-9, SA-9 (2), and SA-9 (3))

[Licensee/Applicant] does the following:
a. Require 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.
b. Define and document oversight and user roles and responsibilities with regard to external information system services.
c. Use automated mechanisms to monitor security control compliance by external service providers on an ongoing basis.
d. Require 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. Establish, document, and maintain trust relationships with external service providers through contracts or service-level agreements to provide assurance that external information system services that interact with VDAs have the security requirements necessary to address the security controls in this appendix.

C-64 Developer Configuration Management
(Informed by NIST SP 800-53, Revision 4, SA-10)

[Licensee/Applicant] requires the developer of the VDA, VDA component, or VDA service to do the following:
a. Perform configuration management during the VDA, component, or service lifecycle.
b. Document, manage, and control the integrity of changes to the VDA, component, or service.
c. Implement only organization-approved changes to the VDA, component, or service.
d. Document approved changes to the VDA, component, or service and the potential security impacts of such changes.
e. Track security flaws and flaw resolution within the VDA, component, or service and report findings to the CST.

C-65 Third-Party Hardware, Software and Firmware

(Informed by NIST SP 800-53, Revision 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 do the following:

a. Create and implement a security assessment plan that includes, at a minimum, the following:
   (1) integrity verification of hardware, software, and firmware components;
   (2) assurance that security-relevant hardware, software, and firmware updates distributed to [Licensee/Applicant] are exactly as specified by the master copies;
   (3) static and dynamic code analysis using tools and techniques that identify common flaws (including manual code review) and documentation of the results of the analysis;
   (4) threat and vulnerability analyses and subsequent testing/evaluation of the as-built VDAs, components, or services;
   (5) full-penetration testing;
   (6) attack surface reviews; and
   (7) verification that the scope of security testing/evaluation provides complete coverage of required security controls.
b. Perform comprehensive cyber security testing and evaluation.
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
d. Implement a verifiable flaw remediation process.
e. Correct flaws identified during security testing/evaluation.

C-66 Developer Security Testing and Evaluation

(Informed by NIST SP 800-53, Revision 4, SA-11)

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

a. Create and implement a security assessment plan.
b. Perform comprehensive cyber security testing and evaluation.
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
d. Implement a verifiable flaw remediation process.
e. Correct flaws identified during security testing/evaluation.

C-67 Enhancements to Supply Chain Protection

(Informed by NIST SP 800-53, Revision 4, SA-12 (1), SA-12 (2), SA-12 (9), SA-12 (10), and SA-12 (14))

[Licensee/Applicant] does the following:

a. Use 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.
b. Conduct a supplier review before entering into a contractual agreement to acquire the VDA, VDA component, or VDA service.
c. Use operations security safeguards in accordance with classification guides to protect supply chain-related information for the VDA, VDA component, or VDA service.
d. Use security safeguards to validate that the VDA received is genuine and has not been altered.
e. Establish and retain 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, Revision 4, SA-13)

When acquiring, designing, developing, or implementing VDAs, [Licensee/Applicant] does the following:

a. Describe the level of required trustworthiness required in the VDA to meet security requirements.
b. Implement measures to achieve, measure, and document such trustworthiness.

C-69 Development Process, Standards, and Tools
(Informed by NIST SP 800-53, Revision 4, SA-15)

[Licensee/Applicant] does the following:

a. Require the developer of the VDA, VDA component, or VDA service to follow a documented development process that does the following:
   (1) explicitly addresses security requirements,
   (2) identifies the standards and tools used in the development process, and
   (3) documents the specific tool options and tool configurations used in the development process.
b. Document, manage, and ensure the integrity of changes to the process or tools, or both, used in development.
c. Review the development process, standards, tools, and tool options/configurations to determine whether the process, standards, tools, and tool options/configurations selected and used can satisfy VDA security requirements.

C-70 Third-Party Developer Process, Standards, and Tools
(Informed by NIST SP 800-53, Revision 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 do the following:

a. Define quality metrics at the beginning of the development process.
b. Provide evidence of meeting the quality metrics upon delivery.
c. Select and use a security tracking tool for use during the development process.
d. Perform a criticality analysis.
e. Perform threat modeling and a vulnerability analysis.
f. Reduce attack surfaces.
g. Implement an explicit process to continuously improve the development process.
h. Perform an automated vulnerability analysis to do the following:
   (1) Determine the exploitation potential for discovered vulnerabilities.
   (2) Determine potential risk mitigations for delivered vulnerabilities.
   (3) 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, Revision 4, SA-17)

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

a. is consistent with and supportive of the licensee's security architecture;
b. accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and

c. 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, Revision 4, SA-17 (1) and SA-17 (2))

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

a. Produce, as an integral part of the development process, a formal policy model describing how security controls in this appendix are met.
b. Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.
c. Define security-relevant hardware, software, and firmware.
d. 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, Revision 4, SA-18, SA-18 (1), and SA-18 (2))

[Licensee/Applicant] does the following:

a. Implement a tamper protection program for the VDA, VDA component, or VDA service.
b. Use antitamper technologies and techniques during multiple phases in the system development life cycle, including design, development, integration, operations, and maintenance.
c. Inspect VDA and VDA components randomly, but at least every hour, to detect tampering.

C-74 Component Authenticity
(Informed by NIST SP 800-53, Revision 4, SA-19)

[Licensee/Applicant] does the following:

a. Develop and implement anticounterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the VDA.
b. Report counterfeit information VDA components to the NRC and relevant law enforcement agencies.
c. Train CST personnel to detect counterfeit information VDA components (including hardware, software, and firmware).
d. Scan for counterfeit information VDA components during VDA validation activities.

C-75 Developer Screening
(Informed by NIST SP 800-53, Revision 4, SA-21 and SA-21 (1))

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

a. Have appropriate access authorizations.
b. Satisfy licensee personnel security requirements.
c. Document, and provide for inspection and assessment, the appropriate access authorizations to ensure that the required access authorizations and screening criteria are satisfied.

C-76 Unsupported VDA Components
(Informed by NIST SP 800-53, Revision 4, SA-22 and SA-22 (1))

[Licensee/Applicant] does the following:

a. Replace information VDA components when support for the components is no longer available from the developer, vendor, or manufacturer.
b. Provide justification and documents approval for the continued use of unsupported VDA components required to satisfy mission/business needs.
c. Retain 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, Revision 4, SC-2, SC-2 (1), SC-3, SC-3 (1), SC-3 (2), and SC-4)

[Licensee/Applicant] does the following:

a. Separate user functionality on the VDA (including user interface services) from VDA management functionality.
b. Isolate security functions from nonsecurity functions on the VDA.
c. Prevent unauthorized and unintended information transfer via shared resources.
d. Prevent the presentation of VDA management-related functionality at an interface for nonprivileged users.
e. Use underlying hardware separation mechanisms to implement security function isolation.
f. Isolate 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, Revision 4, SC-5)

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

C-79 Boundary Protection
(Informed by NIST SP 800-53, Revision 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 that the VDA does the following:

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

[Licensee/Applicant] does the following:

a. Provide the capability to dynamically isolate/segregate VDAs from other VDAs.
b. Prohibit external network connections to the VDA.
c. Protect against unauthorized physical connections to the VDA.
d. Allow only incoming communications from authorized sources to be routed to VDAs.
e. Implement host-based firewalls on VDAs.
f. Protect against unauthorized physical connections to the VDA.
g. Use boundary mechanisms.

[Licensee/Applicant] does the following for boundary control devices:

a. Establish a traffic-flow policy for each interface.
b. Protect the confidentiality and integrity of the information being transmitted across each interface.
c. Document each exception to the traffic-flow policy with a supporting mission/business need and duration of that need.
d. Review exceptions to the traffic-flow policy at least every 30 days and remove exceptions that are no longer supported by an explicit mission/business need.
e. Allow only incoming communications from authorized sources to be routed to VDAs.
f. Implement host-based firewalls on VDAs.
g. Provide the capability to dynamically isolate/segregate VDAs from other VDAs.
h. Ensure that the VDA denies network communications traffic by default and allows network communications traffic by exception (i.e., deny-all, permit-by-exception policy).

C-80 External Telecommunications Services

(Informed by NIST SP 800-53, Revision 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] does the following:

a. Implement a managed interface for each external telecommunication service.
b. Establish a traffic-flow policy for each managed interface.
c. Protect the confidentiality and integrity of the information being transmitted across each interface.
d. Document each exception to the traffic-flow policy with a supporting mission/business need and duration of that need.
e. Review exceptions to the traffic-flow policy on a timely basis and remove exceptions that are no longer supported by an explicit mission/business need.
f. Prevent the unauthorized exfiltration of information across managed interfaces.
g. Allow only incoming communications from authorized sources to be routed to VDAs.
h. Implement host-based firewalls on VDAs.
i. Protect against unauthorized physical connections to the VDA.
j. Use boundary protection mechanisms.

[Licensee/Applicant] ensures that the VDA does the following:

a. has managed interfaces, denies network communications traffic by default, and allows network communications traffic by exception (i.e., deny-all, permit-by-exception policy);
b. prevents, in conjunction with a remote device, the device from simultaneously establishing nonremote connections with the system and communicating via some other connection to resources in external networks;
c. routes internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
d. provides the capability to dynamically isolate/segregate VDAs from other VDAs; and
e. 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, Revision 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures that the VDA does the following:

a. protects the confidentiality and integrity of transmitted information and
b. 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, Revision 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, Revision 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 reauthentication.

[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, Revision 4, SC-12 and SC-12 (1))

[Licensee/Applicant] does the following:

a. Establish and manage cryptographic keys for required cryptography used within the VDA in accordance with the NIST Cryptographic Module Validation Program.
b. Maintain 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, Revision 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 that the VDA does the following:

a. prohibits remote activation of collaborative computing devices except where explicitly authorized,
b. provides an explicit indication of use to users physically present at the devices,
c. provides physical disconnect of collaborative computing devices in a manner that supports ease of use, and
d. provides an explicit indication of current participants in collaborative sessions.

C-86 Public Key Infrastructure Certificates
(Informed by NIST SP 800-53, Revision 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
(Informed by NIST SP 800-53, Revision 4, SC-19)

[Licensee/Applicant] does the following:

a. Establish usage restrictions and implementation guidance for voice over Internet protocol (VoIP) technology based on its potential to cause damage to the VDA if it is used maliciously.
b. Authorize, monitor, and control the use of VoIP within the VDA.

C-88 Secure Name/Address Resolution
(Informed by NIST SP 800-53, Revision 4, SC-20, SC-20a, SC-20 (2), SC-21, and SC-22)

[Licensee/Applicant] ensures that the VDA does the following:

a. provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data that the VDA returns in response to external name/address resolution queries,
b. 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 such domains are operating as part of a distributed hierarchical namespace,
c. requests and performs data origin authentication and data integrity verification on the name/address resolution responses that the VDA receives from authoritative sources,
d. collectively provides a fault-tolerant name/address resolution service for an organization and implements internal/external role separation, and
e. provides data origin and integrity protection artifacts for internal name/address resolution queries.

C-89 Session Authenticity
(Informed by NIST SP 800-53, Revision 4, SC-23)

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

C-90 Fail in Known State
(Informed by NIST SP 800-53, Revision 4, SC-24)

[Licensee/Applicant] does the following:

a. Ensure VDAs fail in a known state to ensure that functions are not adversely impacted.
b. Prevent 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, Revision 4, SC-26)

[Licensee/Applicant] ensures that 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, Revision 4, SC-28)

[Licensee/Applicant] ensures that the VDA does the following:

a. protects the confidentiality and integrity of VDA information at rest and
b. implements cryptographic mechanisms to prevent unauthorized disclosure and modification of VDA information.

C-93 Operations Security
(Informed by NIST SP 800-53, Revision 4, SC-38)

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

C-94 Process Isolation
(Informed by NIST SP 800-53, Revision 4, SC-39)

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

C-95 Port and Input/Output Device Access
(Informed by NIST SP 800-53, Revision 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, Revision 4, SI-2, SI-2 (1), and SI-2 (2))

[Licensee/Applicant] does the following:

a. Identify, report, and correct VDA flaws.
b. Implement temporary compensatory measure following identification of the flaw.
c. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
d. Correct the flaw expeditiously using the configuration management process.
e. Incorporate flaw remediation into the organizational configuration management process.
f. Perform vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production.
g. Centrally manage the flaw remediation process.
h. Use 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, Revision 4, SI-3, SI-3 (1), SI-3 (2), SI-3 (8), and SI-2 (10))

[Licensee/Applicant] does the following:

a. Use malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code.
b. Update malicious code protection mechanisms whenever new releases are available.

c. Configure malicious code protection mechanisms to do the following:
   (1) Perform periodic scans of the VDA at least every 7 days.
   (2) Perform real-time scans of files from external sources as the files are downloaded, opened, or executed.
   (3) Prevent malicious code execution.
   (4) Alert the CST of the detection of malicious code in a timely manner.
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA.
e. Centrally manage malicious code protection mechanisms.
f. Automatically update malicious code protection mechanisms for the VDA.
g. Detect unauthorized operating system commands in VDAs through the kernel application programming interface and do the following:
   (1) Issue a warning.
   (2) Audit the command execution.
   (3) Prevent the execution of the command.
h. Use tools and techniques to analyze the characteristics and behavior of malicious code.
i. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

C-98 VDA Monitoring

(Informed by NIST SP 800-53, Revision 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] does the following:

a. Monitor the VDA to detect the following:
   (1) cyber attacks and indicators of potential cyber attacks, and
   (2) unauthorized local, network, and remote connections.
b. Identify unauthorized use of the VDA using automated or other means.
c. Use internal and external monitoring of VDAs to ensure adequate capability to detect cyber attacks and indicators of compromise.
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
e. Heighten 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.
f. Provide VDA monitoring information to appropriate licensee cyber security personnel as necessary.
g. Use automated tools to support near real-time analysis of events.
h. Monitor inbound and outbound VDA communications traffic in near real time for unusual or unauthorized activities or conditions.
i. Ensure that appropriate cyber security personnel are alerted when indications of a compromise or potential compromise of a VDA occur.
j. Test intrusion-monitoring tools at least every 92 days.
k. Make provisions so that encrypted communications traffic is visible to authorized network monitoring tools.
l. Analyze outbound communications traffic for VDAs at the external boundary and selected interior points within the boundary to discover anomalies.
m. Use automated mechanisms to alert security personnel, in a timely manner, of inappropriate or unusual activities with security implications.
n. Analyze communications traffic/event patterns for the VDA.

o. Develop profiles representing common traffic patterns and/or events.
p. Use the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
q. Use a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the VDA.
r. Use an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
s. Correlate information from monitoring tools used throughout the VDA.
t. Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.
u. Implement additional monitoring of privileged users, probationary personnel, and individuals determined to be high risk.
v. Detect VDA network services that have not been authorized or approved and alert appropriate personnel in a timely manner.
w. Implement host-based monitoring mechanisms.
x. Discover, collect, distribute, and use indicators of VDA compromise.

C-99 Security Alerts, Advisories, and Directives
(Informed by NIST SP 800-53, Revision 4, SI-5 and SI-5 (1))

[Licensee/Applicant] does the following:
a. Receive cyber security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis.
b. Generate internal security alerts, advisories, and directives as necessary to prevent a consequence of concern.
c. Disseminate security alerts, advisories, and directives to appropriate personnel and the NRC.
d. Implement security directives in a timely manner.
e. Use automated mechanisms to make security alert and advisory information available throughout the organization.

C-100 Security Function Verification
(Informed by NIST SP 800-53, Revision 4, SI-6 and SI-6 (3))

[Licensee/Applicant] ensures that the VDA does the following:
a. verifies the correct operation of security functions;
b. performs this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and upon discovery of anomalies; and
c. 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, Revision 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] does the following:
a. Use integrity verification tools to detect unauthorized changes to VDA software, firmware, and information.
b. Perform an integrity check of VDA software, firmware, and information where possible upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and upon discovery of anomalies.

c. Use automated tools that provide notification to appropriate personnel upon discovery of discrepancies during integrity verification.
d. Automatically take proactive protection measures when VDA integrity violations are discovered.
e. Incorporate the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability.
f. Require that the integrity of software be verified before execution.
g. Prohibit 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, Revision 4, SI-10 (3) and SI-10 (5))

[Licensee/Applicant] does the following:
a. Ensure that the VDA behaves in a predictable and documented manner when invalid inputs are received.
b. Restrict the use of information inputs to defined trusted sources and defined formats.

C-103 Error Handling
(Informed by NIST SP 800-53, Revision 4, SI-11)

[Licensee/Applicant] ensures that the VDA does the following:
a. generates VDA error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries, and
b. 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, Revision 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, Revision 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, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, issued April 2013, 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, Revision 4, AC-2)

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

a. Assign account managers for VDA accounts.
b. Establish conditions for group and role membership.
c. Specify authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
d. Require independent management approval for requests to create VDA accounts.
e. Create, enable, modify, disable, and remove VDA accounts in accordance with the access control policy.
f. Monitor the use of VDA accounts.
g. Notify account managers in a timely manner of the following:
   (1) when accounts are no longer required,
   (2) when users are terminated or transferred, and
   (3) when individual VDA usage or need to know changes.
h. Authorize access to the VDA based on the following:
   (1) a valid access authorization, and
   (2) intended VDA usage.
i. Review accounts at least every 30 days for compliance with account management requirements.
j. Take, at a minimum, the following measures to restrict the creation and issuance of shared/group VDA accounts:
   (1) Ensure that each shared/group account request does the following:
      – is issued only when necessary to prevent a consequence of concern,
      – includes a documented technical justification, and
      – is reviewed and approved by the Cyber Security Team (CST) before issuance.
   (2) Automatically terminate and establish 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, Revision 4, AC-2 (5), AC-2 (12), and AC-2 (13))

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

a. Require that users log out within 15 minutes of inactivity unless the login session is required to be maintained to prevent a consequence of concern.
b. Monitor VDA accounts for atypical usage and anomalous activity that could indicate account compromise.
c. Report atypical usage of VDA accounts to the CST.
d. Disable user accounts that have been potentially compromised upon discovery.

D-4 Automated Account Management
(Informed by NIST SP 800-53, Revision 4, AC-2 (1), AC-2 (2), AC-2 (3), and AC-2 (4))

To support the management of VDA accounts, the [Licensee/Applicant] uses, at minimum, automated technical mechanisms that do the following:

a. Automatically remove or disable temporary and emergency accounts once they are no longer needed.
b. Automatically disable inactive accounts within 30 days.
c. Automatically audit account creation, modification, enabling, disabling, and removal actions and notify appropriate personnel in a timely manner.

D-5 Access Management
(Informed by NIST SP 800-53, Revision 4, AC-3 and AC-4)

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

a. logical access to VDA information and VDA resources in accordance with applicable access control policies and
b. control of the flow of information within the VDA and between interconnected systems and VDAs.

D-6 Security Attributes
(Informed by NIST SP 800-53, Revision 4, AC-16, AC-16 (1), AC-16 (4), and SC-16)

[Licensee/Applicant] does the following:

a. Provide the means to associate security attributes with information in storage, in process, and/or in transmission.
b. Ensure that the security attribute associations are made and retained with the information.
c. Establish the permitted security attributes for VDAs.
d. Determine the permitted values or ranges for each of the established security attributes.
e. Support the association of VDA security attributes with information exchanged or transmitted between digital assets, VDAs, and components.
f. Validate the integrity of transmitted security attributes for the VDA.

D-7 Remote Access
(Informed by NIST SP 800-53, Revision 4, AC-17)

[Licensee/Applicant] does the following:

a. Establish and document usage restrictions, configurations, connection requirements, and implementation guidance for each type of remote access allowed.
b. Authorize remote access to the VDA before allowing such connections.

D-8 Managed Access Control Points
(Informed by NIST SP 800-53, Revision 4, AC-17 (3))

[Licensee/Applicant] does the following:

a. Prohibit all remote access to VDAs associated with security functions.
b. Ensure that all remote access to nonsecurity-related VDAs is through a boundary control device that meets the requirements in cyber security control, "Boundary Protection" of this appendix.

D-9 Wireless Access
(Informed by NIST SP 800-53, Revision 4, AC-18)

[Licensee/Applicant] does the following:

a. Establish usage restrictions, configurations, connection requirements, and implementation guidance for wireless access.
b. Authorize wireless access to the VDA before allowing such connections.

D-10 Restrict Configurations by Users
(Informed by NIST SP 800-53, Revision 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, Revision 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, Revision 4, AC-21)

When [Licensee/Applicant] shares VDA information with external parties, it does the following:

a. Ensure that access authorizations assigned to the sharing partner match the access restrictions on the information.
b. Use automated mechanisms to enforce these restrictions.

D-13 Use of External Information Systems
(Informed by NIST SP 800-53, Revision 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 do the following:

a. Access the VDA from external information systems.

b. Process, store, or transmit organization-controlled information using external information systems.

[Licensee/Applicant] does the following:

a. Restrict the use of organization-controlled portable storage devices by authorized individuals on external information systems.
b. Prohibit the use of organization-controlled network accessible storage devices in external information systems.
c. Permit authorized individuals to use an external information system to access the VDA or to process, store, or transmit organization-controlled information only when [Licensee/Applicant] does the following:
   (1) verifies the implementation of security controls on the external system equivalent to security controls addressed for the VDA, or
   (2) 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, Revision 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 that the VDA does the following:

a. 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
b. generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum, the following:
   (1) account (user or service) login failure;
   (2) account role or privilege change;
   (3) file or object creation, modification, and deletion;
   (4) service start and stop;
   (5) privileged service call;
   (6) account creation and modification;
   (7) account right assignment;
   (8) audit policy change;
   (9) user account password change;
   (10) user group creation and modification; and
   (11) remote session start and failure.

[Licensee/Applicant] ensures that the VDA auditing function does the following:

a. alerts cyber security personnel in near real time of an audit processing failure or where audit failure events occur that could indicate VDA compromise,
b. takes automated measures to preserve audit data,
c. provides the capability to increase or modify audit record content in response to threat intelligence,
d. initiates session audits at VDA startup,
e. provides the capability for authorized users to select a user session to capture/record or view/hear,
f. provides the capability for authorized users to capture/record and log content related to a user session, and
g. 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, Revision 4, AU-4, AU-5 (1), AU-9, AU-9 (2), AU-9 (3), AU-9 (4), and AU-10)

[Licensee/Applicant] does the following:

a. Allocate sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configure auditing to prevent exceedance of capacity.
b. Authorize access to management of audit functionality only to authorized users with cyber security responsibilities.
c. Ensure that the VDA provides an alert to authorized personnel when the allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity.
d. Ensure that the VDA backs up audit records onto a physically different VDA rather than the VDA being audited.
e. Ensure that the VDA protects audit information and audit tools from unauthorized access, modification, and deletion.
f. Ensure that the VDA implements cryptographic mechanisms to protect the integrity of audit information and audit tools.
g. Ensure that the VDA protects against an individual (or process acting on behalf of an individual) who falsely denies having performed any action on the VDA.

D-16 Audit Review, Analysis, and Reporting
(Informed by NIST SP 800-53, Revision 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] does the following:

a. Use automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
b. Review and analyze VDA audit records in a timely manner for indications of potential compromise.
c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
d. Integrate 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.
e. Correlate information from audit records with information obtained from monitoring physical access to the VDA to further enhance the ability to identify potential unauthorized activity.
f. Report findings to the CST.
g. Ensure that 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 that the VDA does the following:

a. maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released,
b. validates the binding of the information reviewer identity to the information at the transfer or release points before its release or transfer, and
c. prevents access to and modification or transfer of the information in the event of a validation error.

D-17 Security Control Assessments
(Informed by NIST SP 800-53, Revision 4, CA-2)

[Licensee/Applicant] does the following:

a. Develop a security assessment plan that describes the scope of the assessment, including the following:
   (1) security controls and control enhancements under assessment;
   (2) assessment procedures to be used to determine security control effectiveness; and
   (3) assessment environment, assessment team, and assessment roles and responsibilities.
b. Assess 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.
c. Produce a security assessment report that documents the results of the assessment.
d. Include and document the following as part of the VDA security control assessments:
   (1) an attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
   (2) announced assessments that include the following:
      – 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
      – insider threat assessment (to be done at least every 92 days);
   (3) unannounced assessments (in addition to announced assessments above) that include the following:
      – 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), and
      – performance/load testing (to be done at least every 183 days).
e. Provide the results of the security control assessment to the CST.
f. Restrict 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, Revision 4, CA-2 (1), CA-7 (1), CA-8, and CA-8 (1))

[Licensee/Applicant] does the following:

a. Use 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.
b. Use 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.
c. Conduct penetration testing at least every 12 months on the VDA.
d. Use 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, Revision 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant] does the following:

a. Prohibit remote access to VDAs associated with security functions.

b. Use a "deny-all, permit-by-exception" policy for allowing nonsecurity-related VDAs to connect to external information systems.
c. Prohibit the direct connection of a nonsecurity-related VDA to an external network without the use of the following elements:
   (1) at least one separate, intervening access control device (e.g., firewall and cross-domain solution);
   (2) at least one separate, intervening intrusion detection/prevention mechanism with near real-time prevention, detection, and alerting capability;
   (3) host-based protective measures; and
   (4) other measures necessary to prevent a consequence of concern.
d. Prohibit the direct connection of a VDA to a public network.
e. Authorize connections to the VDA.
f. Document, for each connection, the interface characteristics, security requirements, and nature of the information communicated.

D-20 Temporary Compensatory Measures
(Informed by NIST SP 800-53, Revision 4, CA-5)

[Licensee/Applicant] does the following:
a. Document a temporary 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.
b. Update the temporary compensatory measure plan at least every 30 days based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.
c. Restrict access to the temporary compensatory measure plan to authorized personnel with a need to know.

D-21 Configuration of VDAs for High-Risk Areas
(Informed by NIST SP 800-53, Revision 4, CM-2 (7))

Before transporting VDAs to locations that it considers risk significant, [Licensee/Applicant] does the following:
a. Document a detailed justification for the VDA to be transported.
b. Obtain written approval from the CST and management.
c. Document the VDA configuration baseline and component inventory before it leaves the controlled areas.
d. Ensure safeguards or security-related information on the VDA is purged or protected in a manner that prevents an adversary from recovering the data before it leaves the controlled areas.
e. Perform a review of the VDA configuration baseline and component inventory upon its return.
f. Perform testing of the VDA to ensure no cyber compromise has occurred.
g. Perform a security control assessment to ensure that all controls are in place, operational, and performing their intended function.

D-22 Configuration Change Control
(Informed by NIST SP 800-53, Revision 4, CM-3)

[Licensee/Applicant] does the following:
a. Document changes to the VDA and provide configuration control in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53, "Requirements for Cyber Security at Nuclear Fuel Cycle Facilities."

b. Review proposed configuration-controlled changes to the VDA and approve or disapprove such changes with explicit consideration for security impact analyses before implementing the changes.
c. Document configuration change decisions associated with the VDA.
d. Implement approved configuration-controlled changes to the VDA.
e. Retain records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements.
f. Audit and review activities associated with configuration-controlled changes to the VDA.
g. Coordinate and provide oversight for configuration change control activities through the change management process.

D-23 Change Testing and Analysis
(Informed by NIST SP 800-53, Revision 4, CM-3 (2), CM-4, and CM-4 (1))

[Licensee/Applicant] does the following:
a. Test, validate, and document changes to the VDA before implementing the changes to the VDA.
b. Analyze changes to the VDA to determine potential security impacts before implementing the changes.
c. Analyze 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, Revision 4, CM-5 and CM-5 (1))

[Licensee/Applicant] does the following:
a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the VDA.
b. Ensure that the VDA enforces access restrictions and support auditing of the enforcement actions.

D-25 Review VDA Changes
(Informed by NIST SP 800-53, Revision 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, Revision 4, CM-5 (3))

[Licensee/Applicant] ensures that 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, Revision 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant] does the following:
a. Establish and document configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements.
b. Implement the configuration settings.
c. Identify, document, and approve any deviations from established configuration settings.

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
e. Use automated mechanisms to centrally manage, apply, and verify VDA configuration settings.
f. Report 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, Revision 4, CM-7)

[Licensee/Applicant] does the following:
a. Configure the VDA to provide only essential capabilities to perform its function and maintain safe and secure operations.
b. Prohibit or restrict the use of unneeded functions, ports, protocols, and/or services.

D-29 Periodic Review
(Informed by NIST SP 800-53, Revision 4, CM-7 (1))

[Licensee/Applicant] does the following:
a. Review the VDA at least every 30 days to identify unnecessary and/or nonsecure functions, ports, protocols, and services.
b. Disable or restrict unneeded functions, ports, protocols, and/or services identified by the review.

D-30 Authorized Software
(Informed by NIST SP 800-53, Revision 4, CM-7 (2) and CM-7 (4))

[Licensee/Applicant] does the following:
a. Identify software programs authorized to execute on the VDA.
b. Use a "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA.
c. Review and update the list of authorized software programs at least every 183 days.
d. Use 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, Revision 4, CM-8, CM-8 (1), CM-8 (2), CM-8 (3), and CM-8 (4)

[Licensee/Applicant] does the following:
a. Develop and document an inventory of VDA components that does the following:
   (1) accurately reflects the current VDA,
   (2) includes all components within the boundary of the VDA,
   (3) is at the level of granularity necessary for tracking and reporting, and
   (4) includes information necessary to achieve effective VDA component accountability.
b. Review and update the VDA component inventory at least every 92 days or as part of any changes to a VDA.
c. Update the inventory of VDA components as an integral part of component installations, removals, and VDA updates.
d. Use automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA.
e. Use automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components.

f. Include, in the VDA component inventory information, a means for identifying individuals responsible/accountable for administering those components.
g. Take 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, Revision 4, CM-11)

[Licensee/Applicant] does the following:
a. Establish policies governing the installation of software on VDAs consistent with the configuration management requirements in 10 CFR 73.53(f).
b. Enforce software installation policies using automated measures where supported.
c. Monitor policy compliance using automated measures where supported.

D-33 Identification and Authentication
(Informed by NIST SP 800-53, Revision 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 that the VDA does the following:
a. uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and nonorganizational users (or processes acting on behalf of nonorganizational users);
b. implements multifactor authentication for network access to privileged accounts;
c. implements multifactor authentication for network access to nonprivileged accounts;
d. implements multifactor authentication for local access to privileged accounts;
e. implements multifactor authentication for local access to nonprivileged accounts;
f. implements replay-resistant authentication mechanisms for network access to privileged accounts;
g. implements replay-resistant authentication mechanisms for network access to nonprivileged accounts;
h. implements multifactor authentication for remote access to privileged and nonprivileged accounts such that a device separate from the VDA gaining access provides one of the factors and that the device meets e-authentication assurance Level 3 as described in NIST SP 800-63-2, "Electronic Authentication Guideline," issued August 2013, or later revisions;
i. accepts and electronically verifies personal identity verification credentials; and
j. uniquely identifies and authenticates devices before establishing a connection to a VDA.

D-34 Identifier Management
(Informed by NIST SP 800-53, Revision 4, IA-4)

[Licensee/Applicant] manages VDA identifiers by doing the following:
a. receiving independent management authorization to assign an individual, group, role, or device identifier;
b. selecting an identifier that identifies an individual, group, role, or device;
c. assigning the identifier to the intended individual, group, role, or device;
d. preventing reuse of identifiers where reuse could allow unintended or unauthorized access; and
e. disabling the identifier within 30 days of inactivity.

D-35 Authenticator Management
(Informed by NIST SP 800-53, Revision 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by doing the following:

a. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. establishing initial authenticator content for authenticators defined by the organization;
c. ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. establishing and implementing administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revocation of authenticators;
e. changing default content of authenticators before VDA installation;
f. establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. documenting authenticator types approved for use, the frequency for changing/refreshing them, and the technical justification that demonstrates that this frequency provides adequate security;
h. protecting authenticator content from unauthorized disclosure and modification;
i. requiring individuals to take, and to have devices implement, specific security safeguards to protect authenticators; and
j. changing authenticators for group/role accounts when membership to those accounts changes.

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

D-36 Password-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (1))

For password-based authentication for the VDA, [Licensee/Applicant] does the following:

a. Enforce a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security.
b. Enforce password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters.
c. Enforce a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries.
d. Store and transmit only cryptographically protected passwords.
e. Enforce lifetime restrictions for password minimums of 1 day and provide a technical basis for maximums defined and documented by the CST that prevents unauthorized access.
f. Prohibit password reuse for 10 generations.
g. Require an immediate change to a permanent password upon the first logon when temporary passwords are used for VDA logons.
h. Store written or electronic copies of master passwords in a secure location with limited access.

D-37 Public Key Infrastructure-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (2))

[Licensee/Applicant] ensures that the public key infrastructure-based authentication for the VDA does the following:

a. validates certifications by constructing and verifying a certification path to an accepted trust anchor and by checking certificate status information,
b. enforces authorized access to the corresponding private key,
c. maps the authenticated identity to the account of the individual or group, and
d. implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information through the network.

D-38 In-Person or Trusted Third-Party Registration
(Informed by NIST SP 800-53, Revision 4, IA-5 (3))

[Licensee/Applicant] requires the registration process for receiving authenticators to 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, Revision 4, IA-5 (11))

[Licensee/Applicant] ensures that hardware token-based authentication for the VDA uses 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, Revision 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.

D-41 Cryptographic Module Authentication
(Informed by NIST SP 800-53, Revision 4, IA-7)

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

D-42 Incident Response Training
(Informed by NIST SP 800-53, Revision 4, IR-2, IR-2 (1), and IR-2 (2))

[Licensee/Applicant] provides incident response training to VDA users consistent with their assigned roles and responsibilities as follows:
a. within 92 days of assuming an incident response role or responsibility,
b. when required by VDA changes, and
c. at least every 12 months.

[Licensee/Applicant] does the following:
a. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
b. Use automated mechanisms to provide a more thorough and realistic incident response training environment.

D-43 Incident Response Testing
(Informed by NIST SP 800-53, Revision 4, IR-3 and IR-3 (2))

[Licensee/Applicant] does the following:
a. Test 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 document the results of checklists, walkthrough or tabletop exercises, and simulations (parallel/full interrupt).
b. Test the incident response capability for the VDA at least every 36 months using a comprehensive exercise.

c. Coordinate incident response testing with organizational elements responsible for related plans.

D-44 Incident Handling
(Informed by NIST SP 800-53, Revision 4, IR-4, IR-4 (1), and IR-4 (4))

[Licensee/Applicant] does the following:

a. Implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
b. Coordinate incident-handling activities with contingency planning activities.
c. Incorporate lessons learned from ongoing incident-handling activities into incident response procedures, training, and testing and implement the resulting changes accordingly.
d. Use automated mechanisms to support the incident-handling process.
e. Correlate 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, Revision 4, IR-5 and IR-5 (1))

[Licensee/Applicant] does the following:

a. Track and document VDA security incidents.
b. Use 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, Revision 4, IR-6 and IR-6 (1))

[Licensee/Applicant] does the following:

a. Require personnel to report suspected cyber security incidents to the CST upon discovery.
b. Use automated mechanisms to assist in the reporting of security incidents.

D-47 Incident Response Assistance
(Informed by NIST SP 800-53, Revision 4, IR-7 and IR-7 (1))

[Licensee/Applicant] does the following:

a. Provide 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.
b. Use automated mechanisms to increase the availability of incident response-related information and support.

D-48 Information Spillage Response
(Informed by NIST SP 800-53, Revision 4, IR-9, IR-9 (1), IR-9 (2), IR-9 (3), and IR-9 (4))

[Licensee/Applicant] does the following:

a. Respond to information spills by doing the following:
   (1) identifying the specific information involved in the VDA contamination,
   (2) alerting the CST of the information spill using a method of communication not associated with the spill,
   (3) isolating the contaminated VDA or system component,
   (4) eradicating the information from the contaminated VDA or component,

(5) identifying other VDAs or system components that may have been subsequently contaminated, and
(6) documenting the incident.

b. Assign authorized personnel with responsibility for responding to information spills.
c. Provide information spillage response training at least every 12 months.
d. Implement procedures to ensure that corrective actions associated with information spills cannot result in consequence of concern.
e. Use appropriate response procedures and safeguards for personnel exposed to information that is not within their assigned access authorizations.

D-49 Controlled Maintenance
(Informed by NIST SP 800-53, Revision 4, MA-2 and MA-2 (2))

[Licensee/Applicant] does the following:

a. Perform and document maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern.
b. Review records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days.
c. Approve and monitor all maintenance activities whether these activities are performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.
d. Require the CST to approve the removal of the VDA for offsite maintenance or repairs outside the licensee's positive control.
e. Sanitize equipment to remove all information from associated media before removal for offsite maintenance or repairs outside the licensee's positive control.
f. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
g. Include in records of maintenance and repairs on VDA components, at a minimum, the date, time, identification of those performing the maintenance, description of maintenance performed, and list of VDA components removed or replaced.
h. Retain records for inspection by the NRC.
i. Use automated mechanisms to schedule, conduct, and document maintenance and repairs.
j. Produce 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, Revision 4, MA-3, MA-3 (1), and MA-3 (2), and MA-3 (3))

[Licensee/Applicant] does the following:

a. Approve, control, and monitor VDA maintenance tools.
b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
c. Check 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 doing the following:

a. verifying that there is no VDA information contained on the equipment,
b. sanitizing or destroying the equipment,
c. retaining the equipment within the facility, or
d. 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, Revision 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant] does the following:

a. Approve and monitor nonlocal maintenance and diagnostic activities.
b. Document and only allow 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).
c. Use strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.
d. Maintain records for nonlocal maintenance and diagnostic activities.
e. Terminate session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant] does one the following:

a. Document the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
b. Remove the component to be serviced from the VDA before using nonlocal maintenance or diagnostic services; sanitize the component (with regard to VDA information) before removing it from licensee facilities; and, after the service is performed, inspect and sanitize the component (with regard to potentially malicious software) before reconnecting it to the VDA.

D-52 Maintenance Personnel
(Informed by NIST SP 800-53, Revision 4, MA-5 and MA-5 (1))

[Licensee/Applicant] does the following:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
b. Ensure that unescorted personnel performing maintenance on the VDA have the required access authorizations.
c. Designate 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] does the following:

a. Implement procedures for the use of maintenance personnel who lack appropriate security clearances that include the following requirements:
    (1) Approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified escort and supervise maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals during the performance of maintenance and diagnostic activities on the VDA.
    (2) Before 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.
b. Develop and implement alternate security safeguards in the event that a VDA component cannot be sanitized, removed, or disconnected from the VDA.

D-53 Timely Maintenance
(Informed by NIST SP 800-53, Revision 4, MA-6)

[Licensee/Applicant] obtains maintenance support or spare parts, or both, for VDAs that are required to remain operational to prevent a consequence of concern.

D-54 Media Access
(Informed by NIST SP 800-53, Revision 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media include any active storage device, passive storage device, or passive media that have one of the following characteristics:

a. They contain information used to manage, configure, maintain, secure, or operate the VDA.
b. They are used on the VDA for any purpose.

D-55 Media Marking
(Informed by NIST SP 800-53, Revision 4, MP-3)

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

D-56 Media Storage
(Informed by NIST SP 800-53, Revision 4, MP-4)

[Licensee/Applicant] does the following:

a. Physically control and securely store VDA media.
b. Protect 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, Revision 4, MP-5 and MP-5 (4))

[Licensee/Applicant] does the following:

a. Protect and control VDA media during transport outside of controlled areas.
b. Maintain accountability for VDA media during transport outside of controlled areas.
c. Document activities associated with the transport of VDA media.
d. Restrict the activities associated with the transport of VDA media to authorized personnel.
e. Implement 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, Revision 4, MP-6, MP-6 (1), MP-6 (2), and MP-6 (3))

[Licensee/Applicant] does the following:

a. Sanitize VDA media before disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary.
b. Review, approve, track, document, and verify media sanitization and disposal actions.
c. Use sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
d. Test sanitization equipment and procedures at least every 12 months to verify that the intended sanitization is being achieved.

e. Apply nondestructive sanitization techniques to portable storage devices before connecting such devices to the VDA.

D-59 Media Use
(Informed by NIST SP 800-53, Revision 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, Revision 4, PE-6)

[Licensee/Applicant] does the following:

a. Monitor physical access to the facility where the VDA resides to detect and respond to physical security incidents.
b. Review physical access logs in a timely manner and upon occurrence of anomalous behavior.
c. Coordinate results of reviews and investigations with the organizational incident response capability.
d. Monitor physical access to the VDA to detect unauthorized access in a timely manner.

D-61 Vulnerability Scanning
(Informed by NIST SP 800-53, Revision 4, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), and RA-5 (5))

[Licensee/Applicant] does the following:

a. Scan for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA or applications, or both, are identified and reported.
b. Use vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards that require the following:
   (1) enumeration of platforms, software flaws, and improper configurations;
   (2) formatting of checklists and test procedures; and
   (3) measurement of vulnerability impact.
c. Analyze vulnerability scan reports and results from security control assessments.
d. Address vulnerabilities in a timely and technically justified manner to prevent a consequence of concern.
e. Share 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).
f. Use vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned.
g. Update the VDA vulnerabilities scanned before performing a new scan.
h. Use vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information VDA components scanned and vulnerabilities checked).
i. Determine what information about the VDA is discoverable by adversaries and take measures to address the associated potential cyber security issues.
j. Implement privileged access authorization to the VDA for vulnerability scanning activities.

D-62 External Information System Services
(Informed by NIST SP 800-53, Revision 4, SA-9 and SA-9 (2))

[Licensee/Applicant] does the following:

a. Require providers of external information system services that interact with VDAs to comply with information security requirements and to address security controls for the associated consequence of concern.
b. Define and document oversight and user roles and responsibilities with regard to external information system services.
c. Use automated mechanisms to monitor security control compliance by external service providers on an ongoing basis.
d. Require 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, Revision 4, SA-10)

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

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

D-64 Developer Security Testing and Evaluation
(Informed by NIST SP 800-53, Revision 4, SA-11)

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

a. Create and implement a security assessment plan.
b. Perform comprehensive cyber security testing and evaluation.
c. Produce evidence of the execution of the security assessment plan and the results of the security testing and evaluation.
d. Implement a verifiable flaw remediation process.
e. Correct flaws identified during security testing and evaluation.

D-65 Development Process, Standards, and Tools
(Informed by NIST SP 800-53, Revision 4, SA-15)

[Licensee/Applicant] does the following:

a. Require the developer of the VDA, VDA component, or VDA service to follow a documented development process that does the following:
    (1) explicitly addresses security requirements,
    (2) identifies the standards and tools used in the development process, and
    (3) documents the specific tool options and tool configurations used in the development process.
b. Document, manage, and ensure the integrity of changes to the process or tools, or both, used in development.

c. Review the development process, standards, tools, and tool options/configurations to determine whether the process, standards, tools, and tool options/configurations selected and used can satisfy VDA security requirements.

D-66 Developer Security Architecture and Design
(Informed by NIST SP 800-53, Revision 4, SA-17)

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

a. is consistent with and supportive of the licensee's security architecture;
b. accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and
c. 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, Revision 4, SC-2, SC-3, and SC-4)

[Licensee/Applicant] does the following:

a. Separate user functionality on the VDA (including user interface services) from VDA management functionality.
b. Isolate security functions from nonsecurity functions on the VDA.
c. Prevent unauthorized and unintended information transfer through shared resources.

D-68 Denial of Service Protection
(Informed by NIST SP 800-53, Revision 4, SC-5)

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

D-69 Boundary Protection
(Informed by NIST SP 800-53, Revision 4, SC-7, SC-7 (3), SC-7 (4), SC-7 (5), and SC-7 (7))

[Licensee/Applicant] ensures that the VDA does the following:

a. monitors and controls communications at the boundary of the VDA and at key internal boundaries within the VDA,
b. implements subnetworks for publicly or externally accessible VDA components that are physically or logically separated from internal [Licensee/Applicant] networks, and
c. 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, Revision 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] does the following:

a. Implement a managed interface for each external telecommunication service.
b. Establish a traffic-flow policy for each managed interface.
c. Protect the confidentiality and integrity of the information being transmitted across each interface.

d. Document each exception to the traffic-flow policy with a supporting mission/business need and duration of that need.
e. Review exceptions to the traffic-flow policy on a timely basis and remove exceptions that are no longer supported by an explicit mission/business need.
f. Prevent the unauthorized exfiltration of information across managed interfaces.
g. Allow only incoming communications from authorized sources to be routed to VDAs.
h. Implement host-based firewalls on VDAs.
i. Protect against unauthorized physical connections to the VDA.
j. Use boundary mechanisms.

[Licensee/Applicant] ensures that the VDA does the following:
a. has managed interfaces, denies network communications traffic by default, and allows network communications traffic by exception (i.e., deny-all, permit-by-exception policy);
b. prevents, in conjunction with a remote device, the device from simultaneously establishing nonremote connections with the system and communicating through some other connection to resources in external networks;
c. routes internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
d. provides the capability to dynamically isolate/segregate VDAs from other VDAs; and
e. 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, Revision 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures that the VDA does the following:
a. protects the confidentiality and integrity of transmitted information and
b. 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, Revision 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 that are necessary to prevent a consequence of concern.

D-73 Cryptographic Key Establishment and Management
(Informed by NIST SP 800-53, Revision 4, SC-12 and SC-12 (1))

[Licensee/Applicant] does the following:
a. Establish and manage cryptographic keys for required cryptography used within the VDA in accordance with the NIST Cryptographic Module Validation Program.
b. Maintain availability of information necessary to safely operate the VDA or to 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, Revision 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 that the VDA does the following:

a. prohibits remote activation of collaborative computing devices except where explicitly authorized,
b. provides an explicit indication of use to users physically present at the devices,
c. provides physical disconnect of collaborative computing devices in a manner that supports ease of use, and
d. provides an explicit indication of current participants in collaborative sessions.

D-75 Public Key Infrastructure Certificates
(Informed by NIST SP 800-53, Revision 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
(Informed by NIST SP 800-53, Revision 4, SC-19)

[Licensee/Applicant] does the following:

a. Establish usage restrictions and implementation guidance for voice over Internet protocol (VoIP) technology based on its potential to cause damage to the VDA if it is used maliciously.
b. Authorize, monitor, and control the use of VoIP within the VDA.

D-77 Secure Name/Address Resolution
(Informed by NIST SP 800-53, Revision 4, SC-20, SC-20a, SC-21, and SC-22)

[Licensee/Applicant] ensures that the VDA does the following:

a. provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data that the VDA returns in response to external name/address resolution queries,
b. 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 such domains are operating as part of a distributed hierarchical namespace,
c. requests and performs data origin authentication and data integrity verification on the name/address resolution responses that the VDA receives from authoritative sources, and
d. collectively provides a fault-tolerant name/address resolution service for an organization and implements internal/external role separation.

D-78 Session Authenticity
(Informed by NIST SP 800-53, Revision 4, SC-23)

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

D-79 Fail in Known State
(Informed by NIST SP 800-53, Revision 4, SC-24)

[Licensee/Applicant] does the following:

a. Ensure that VDAs fail in a known state to ensure that functions are not adversely impacted.
b. Prevent 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, Revision 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, Revision 4, SC-39)

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

D-82 Flaw Remediation
(Informed by NIST SP 800-53, Revision 4, SI-2 and SI-2 (2))

[Licensee/Applicant] does the following:

a. Identify, report, and correct VDA flaws.
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
c. Correct the flaw expeditiously using the configuration management process.
d. Incorporate flaw remediation into the organizational configuration management process.
e. Perform vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production.
f. Use 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, Revision 4, SI-3, SI-3 (1), SI-3 (2), SI-3 (8), and SI-3 (10))

[Licensee/Applicant] does the following:

a. Use malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code.
b. Update malicious code protection mechanisms whenever new releases are available.
c. Configure malicious code protection mechanisms to do the following:
    (1) Perform periodic scans of the VDA at least every 7 days.
    (2) Perform real-time scans of files from external sources as the files are downloaded, opened, or executed.
    (3) Prevent malicious code execution.
    (4) Alert the CST of the detection of malicious code in a timely manner.
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA.
e. Centrally manage malicious code protection mechanisms.
f. Automatically update malicious code protection mechanisms for the VDA.
g. Detect unauthorized operating system commands in VDAs through the kernel application programming interface and do the following:

(1) Issue a warning.
(2) Audit the command execution.
(3) Prevent the execution of the command.

h. Use tools and techniques to analyze the characteristics and behavior of malicious code.

i. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

D-84 VDA Monitoring

(Informed by NIST SP 800-53, Revision 4, SI-4, SI-4 (2), SI-4 (4), and SI-4 (5))

[Licensee/Applicant] does the following:

a. Monitor the VDA to detect the following:
(1) cyber attacks and indicators of potential cyber attacks and
(2) unauthorized local, network, and remote connections.

b. Identify unauthorized use of the VDA using automated or other means.

c. Deploy monitoring devices as follows:
(1) strategically within the VDA to collect organization-determined essential information and
(2) at ad hoc locations within the system to track specific types of transactions of interest to the organization.

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Heighten 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.

f. Provide VDA monitoring information to appropriate licensee cyber security personnel as necessary.

g. Use automated tools to support near real-time analysis of events.

h. Monitor inbound and outbound communications traffic for the VDA in near real time for unusual or unauthorized activities or conditions.

i. Ensure that 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, Revision 4, SI-5 and SI-5 (1))

[Licensee/Applicant] does the following:

a. Receive cyber security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis.

b. Generate internal security alerts, advisories, and directives as necessary to prevent a consequence of concern.

c. Disseminate security alerts, advisories, and directives to appropriate personnel and the NRC.

d. Implement security directives in a timely manner.

e. Use automated mechanisms to make security alert and advisory information available throughout the organization.

D-86 Security Function Verification

(Informed by NIST SP 800-53, Revision 4, SI-6 and SI-6 (3))

[Licensee/Applicant] does the following:

a. Verify the correct operation of security functions.

b. Perform this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and upon the discovery of anomalies.
c. Notify appropriate personnel in a timely manner of failed security verification tests.
d. Report the results of security function verification to the CST.

D-87 Software, Firmware, and Information Integrity
(Informed by NIST SP 800-53, Revision 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] does the following:
a. Use integrity verification tools to detect unauthorized changes to VDA software, firmware, and information.
b. Perform an integrity check of VDA software, firmware, and information where possible upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and upon discovery of anomalies.
c. Use automated tools that provide notification to appropriate personnel upon discovering discrepancies during integrity verification.
d. Automatically take proactive protection measures when VDA integrity violations are discovered.
e. Incorporate the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability.
f. Require that the integrity of software be verified before its execution.
g. Prohibit 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, Revision 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, Revision 4, SI-11)

[Licensee/Applicant] ensures that the VDA does the following:
a. generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries, and
b. reveals error messages only to authorized personnel with a need to know.

D-90 Information Handling and Retention
(Informed by NIST SP 800-53, Revision 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, Revision 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, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, issued April 2013, AC-2)

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

a. Assign account managers for VDA accounts.
b. Establish conditions for group and role membership.
c. Specify authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
d. Require independent management approval for requests to create VDA accounts.
e. Create, enable, modify, disable, and remove VDA accounts in accordance with the access control policy.
f. Monitor the use of VDA accounts.
g. Notify account managers in a timely manner of the following:
   (1) when accounts are no longer required,
   (2) when users are terminated or transferred, and
   (3) when individual VDA usage or need-to-know changes.
h. Authorize access to the VDA based on the following:
   (1) a valid access authorization and
   (2) intended VDA usage.
i. Review accounts at least every 30 days for compliance with account management requirements.
j. Take, at a minimum, the following measures to restrict the creation and issuance of shared/group VDA accounts:
   (1) Ensure that each shared/group account request does the following:
      – is issued only when necessary to prevent a consequence of concern,
      – includes a documented technical justification, and
      – is reviewed and approved by the Cyber Security Team (CST) before issuance.
   (2) Automatically terminate and establish 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, Revision 4, AC-2 (5), AC-2 (12), and AC-2 (13))

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

a. Require that users log out within 15 minutes of inactivity unless the login session is required to be maintained to prevent a consequence of concern.
b. Monitor VDA accounts for atypical usage and anomalous activity that could indicate account compromise.
c. Report atypical usage of VDA accounts to the CST.

d. Disable user accounts that have been potentially compromised upon discovery.

E-3 Automated Account Management
(Informed by NIST SP 800-53, Revision 4, AC-2 (1), AC-2 (2), AC-2 (3), and AC-2 (4))

To support the management of VDA accounts, [Licensee/Applicant] uses, at a minimum, automated technical mechanisms that do the following:

a. Automatically remove or disable temporary and emergency accounts once they are no longer needed.
b. Automatically disable inactive accounts within 30 days.
c. Automatically audit account creation, modification, enabling, disabling, and removal actions and notify appropriate personnel in a timely manner.

E-4 Access Management
(Informed by NIST SP 800-53, Revision 4, AC-3 and AC-4)

[Licensee/Applicant] ensures that VDAs use technical measures in support of the enforcement of account access to enforce approved authorizations for the following:

a. logical access to VDA information and VDA resources in accordance with applicable access control policies and
b. control of the flow of information within the VDA and between interconnected systems and VDAs.

E-5 Remote Access
(Informed by NIST SP 800-53, Revision 4, AC-17)

[Licensee/Applicant] does the following:

a. Establish and document usage restrictions, configurations, connection requirements, and implementation guidance for each type of remote access allowed.
b. Authorize remote access to the VDA before allowing such connections.

E-6 Managed Access Control Points
(Informed by NIST SP 800-53, Revision 4, AC-17 (3))

[Licensee/Applicant] ensures that all remote access to VDAs is through a boundary control device that meets the cyber security control requirements in "Boundary Protection," of this appendix.

E-7 Wireless Access
(Informed by NIST SP 800-53, Revision 4, AC-18)

[Licensee/Applicant] does the following:

a. Establish usage restrictions, configurations, connection requirements, and implementation guidance for wireless access.
b. Authorize wireless access to the VDA before allowing such connections.

E-8 Restrict Configurations by Users
(Informed by NIST SP 800-53, Revision 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, Revision 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, Revision 4, AC-21)

When [Licensee/Applicant] shares VDA information with external parties, it does the following:

a. Ensure that access authorizations assigned to the sharing partner match the access restrictions on the information.
b. Use automated mechanisms to enforce these restrictions.

E-11 Use of External Information Systems
(Informed by NIST SP 800-53, Revision 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 do the following:

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

[Licensee/Applicant] does the following:

a. Restrict the use of organization-controlled portable storage devices by authorized individuals on external information systems.
b. Permit authorized individuals to use an external information system to access the VDA or to process, store, or transmit organization-controlled information only when [Licensee/Applicant] does the following:
   (1) verifies the implementation of security controls on the external system equivalent to security controls addressed for the VDA, or
   (2) 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, Revision 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 that the VDA does the following:

a. generates records containing information that establishes what type of event that 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
b. generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum, the following:
   (1) account (user or service) login failure;
   (2) account role or privilege change;
   (3) file or object creation, modification, and deletion;
   (4) service start and stop;
   (5) privileged service call;
   (6) account creation and modification;

(7) account right assignment;
(8) audit policy change;
(9) user account password change;
(10) user group creation and modification; and
(11) remote session start and failure.

[Licensee/Applicant] ensures that the VDA auditing function does the following:

a. alerts cyber security personnel in near real time of an audit processing failure or where audit failure events occur that could indicate VDA compromise,
b. takes automated measures to preserve audit data,
c. provides the capability to increase or modify audit record content in response to threat intelligence,
d. initiates session audits at VDA startup,
e. provides the capability for authorized users to select a user session to capture/record or view/hear,
f. provides the capability for authorized users to capture/record and log content related to a user session, and
g. 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, Revision 4, AU-4, AU-5 (1), AU-9, AU-9 (2), AU-9 (3), AU-9 (4), and AU-10)

[Licensee/Applicant] does the following:

a. Allocate sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configure auditing to prevent exceedance of capacity.
b. Authorize access to management of audit functionality only to authorized users with cyber security responsibilities.
c. Ensure that the VDA provides an alert to authorized personnel when the allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity.
d. Ensure that the VDA backs up audit records onto a physically different VDA rather than the VDA being audited.
e. Ensure that the VDA protects audit information and audit tools from unauthorized access, modification, and deletion.
f. Ensure that the VDA implements cryptographic mechanisms to protect the integrity of audit information and audit tools.
g. Ensure that the VDA protects against an individual (or process acting on behalf of an individual) who falsely denies having performed any action on the VDA.

E-14 Audit Review, Analysis, and Reporting
(Informed by NIST SP 800-53, Revision 4, AU-6, AU-6 (1), AU-6 (3), AU-6 (5), AU-6 (6), and AU-12 (1))

[Licensee/Applicant] does the following:

a. Use automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
b. Review and analyze VDA audit records in a timely manner for indications of potential compromise.
c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

d. Integrate 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.
e. Correlate information from audit records with information obtained from monitoring physical access to the VDA to further enhance the ability to identify potential unauthorized activity.
f. Report findings to the CST.
g. Ensure that the VDA compiles audit records into a logical or physical audit trail that is time correlated to within one-tenth of a second at a minimum.

E-15 Security Control Assessments
(Informed by NIST SP 800-53, Revision 4, CA-2 (2))

[Licensee/Applicant] includes and documents the following as part of VDA security control assessments:
a. an attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
b. announced assessments that include the following:
   (1) in-depth monitoring (to be done automatically in real time),
   (2) vulnerability scanning (to be done at least every 30 days), and
   (3) malicious actor testing (to be done at least every 92 days); and
c. unannounced assessments (in addition to announced assessments above) that include the following:
   (1) vulnerability scanning (to be done at least every 183 days),
   (2) malicious actor testing (to be done at least every 12 months), and
   (3) performance/load testing (to be done at least every 183 days).

E-16 Independence of Assessors
(Informed by NIST SP 800-53, Revision 4, CA-2 (1), CA-7 (1), CA-8, and CA-8 (1))

[Licensee/Applicant] does the following:
a. Use 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.
b. Use 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.
c. Conduct penetration testing at least every 12 months on the VDA.
d. Use 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, Revision 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant] does the following:
a. Use a “deny-all, permit-by-exception” policy for allowing VDAs to connect to external information systems.
b. Prohibit the direct connection of a VDA to an external network without the use of the following:
   (1) at least one separate, intervening access control device (e.g., firewall and cross-domain solution);
   (2) at least one separate, intervening intrusion detection/prevention mechanism with near real-time prevention, detection, and alerting capability;

(3) host-based protective measures; and
(4) other measures necessary to prevent a consequence of concern.

c. Prohibit the direct connection of a VDA to a public network.
d. Authorize connections to the VDA.
e. Document, for each connection, the interface characteristics, security requirements, and nature of the information communicated.

E-18 Automated Baseline Configuration
(Informed by NIST SP 800-53, Revision 4, CM-2 (2))

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

E-19 Configuration of VDAs for High-Risk Areas
(Informed by NIST SP 800-53, Revision 4, CM-2 (7))

Before transporting VDAs associated with an active consequence of concern to locations that it considers risk significant, [Licensee/Applicant] should do the following:

a. Document a detailed justification for the VDA to be transported.
b. Obtain written approval from the CST and management.
c. Document the VDA configuration baseline and component inventory before leaving controlled areas.
d. Observe chain of custody of the VDA or VDA component.
e. Perform a review of the VDA configuration baseline and component inventory upon return.
f. Perform testing of the VDA to ensure no cyber compromise has occurred.
g. Perform 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, Revision 4, CM-3)

[Licensee/Applicant] does the following:

a. Document changes to the VDA and provide configuration control in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53, "Requirements for Cyber Security at Nuclear Fuel Cycle Facilities."
b. Review proposed configuration-controlled changes to the VDA and approve or disapprove such changes with explicit consideration for security impact analyses before implementing the changes.
c. Document configuration change decisions associated with the VDA.
d. Implement approved configuration-controlled changes to the VDA.
e. Retain records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements.
f. Audit and review activities associated with configuration-controlled changes to the VDA.
g. Coordinate and provide oversight for configuration change control activities through the change management process.

E-21 Change Testing and Analysis
(Informed by NIST SP 800-53, Revision 4, CM-3 (2), CM-4, and CM-4 (1))

[Licensee/Applicant] does the following:

a. Test, validate, and document changes to the VDA before implementing the changes to the VDA.

b. Analyze changes to the VDA to determine potential security impacts before implementing the changes.
c. Analyze changes to the VDA in a separate test environment before implementing the changes in an operational environment and look for security impacts caused by flaws, weaknesses, incompatibility, or intentional malice.

E-22 Access Restrictions for Change
(Informed by NIST SP 800-53, Revision 4, CM-5 and CM-5 (1))

[Licensee/Applicant] does the following:
a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the VDA.
b. Ensure that the VDA enforces access restrictions and support auditing of the enforcement actions.

E-23 Review VDA Changes
(Informed by NIST SP 800-53, Revision 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, Revision 4, CM-5 (3))

[Licensee/Applicant] ensures that 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, Revision 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant] does the following:
a. Establish and document configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements.
b. Implement the configuration settings.
c. Identify, document, and approve any deviations from established configuration settings.
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
e. Use automated mechanisms to centrally manage, apply, and verify VDA configuration settings.
f. Report 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, Revision 4, CM-7)

[Licensee/Applicant] does the following:
a. Configure the VDA to provide only essential capabilities to perform its function and maintain safe and secure operations.
b. Prohibit or restrict the use of unneeded functions, ports, protocols, and/or services.

E-27 Periodic Review
(Informed by NIST SP 800-53, Revision 4, CM-7 (1))

[Licensee/Applicant] does the following:

a. Review the VDA at least every 30 days to identify unnecessary and/or nonsecure functions, ports, protocols, and services.
b. Disable or restrict unneeded functions, ports, protocols, and/or services identified by the review.

E-28 Authorized Software
(Informed by NIST SP 800-53, Revision 4, CM-7 (2) and CM-7 (4))

[Licensee/Applicant] does the following:

a. Identify software programs authorized to execute on the VDA.
b. Use a "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA.
c. Review and update the list of authorized software programs at least every 183 days.
d. Use 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, Revision 4, CM-8, CM-8 (1), CM-8 (2), CM-8 (3), and CM-8 (4)

[Licensee/Applicant] does the following:

a. Develop and document an inventory of VDA components that does the following:
   (1) accurately reflects the current VDA,
   (2) includes all components within the boundary of the VDA,
   (3) is at the level of granularity necessary for tracking and reporting, and
   (4) includes information necessary to achieve effective VDA component accountability.
b. Review and update the VDA component inventory at least every 92 days or as part of any changes to a VDA.
c. Update the inventory of VDA components as an integral part of component installations, removals, and VDA updates.
d. Use automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA.
e. Use automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of VDA components.
f. Include, in the VDA component inventory information, a means for identifying individuals responsible/accountable for administering those components.
g. Take 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, Revision 4, CM-11)

[Licensee/Applicant] does the following:

a. Establish policies governing the installation of software on VDAs consistent with the configuration management requirements in 10 CFR 73.53(f).
b. Enforce software installation policies using automated measures where supported.
c. Monitor policy compliance using automated measures where supported.

E-31 Identification and Authentication

(Informed by NIST SP 800-53, Revision 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 that the VDA does the following:

a. uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and nonorganizational users (or processes acting on behalf of non-organizational users);
b. implements multifactor authentication for network access to privileged accounts;
c. implements multifactor authentication for network access to nonprivileged accounts;
d. implements multifactor authentication for local access to privileged accounts;
e. implements multifactor authentication for local access to nonprivileged accounts;
f. implements replay-resistant authentication mechanisms for network access to privileged accounts;
g. implements replay-resistant authentication mechanisms for network access to nonprivileged accounts;
h. implements multifactor authentication for remote access to privileged and nonprivileged accounts such that a device separate from the VDA gaining access provides one of the factors and that the device meets e-authentication assurance Level 3 as described in NIST SP 800-63-2, "Electronic Authentication Guideline," issued August 2013, or later revisions;
i. accepts and electronically verifies personal identity verification credentials; and
j. uniquely identifies and authenticates devices before establishing a connection to a VDA.

E-32 Identifier Management

(Informed by NIST SP 800-53, Revision 4, IA-4)

[Licensee/Applicant] does the following to manage VDA identifiers:

a. Receive independent management authorization to assign an individual, group, role, or device identifier.
b. Select an identifier that identifies an individual, group, role, or device.
c. Assign the identifier to the intended individual, group, role, or device.
d. Prevent reuse of identifiers where reuse could allow unintended or unauthorized access.
e. Disable the identifier within 30 days of inactivity.

E-33 Authenticator Management

(Informed by NIST SP 800-53, Revision 4, IA-5)

[Licensee/Applicant] does the following to manage VDA authenticators:

a. Verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
b. Establish initial authenticator content for authenticators defined by the organization.
c. Ensure that authenticators have sufficient strength of mechanism for their intended use.
d. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revocation of authenticators.
e. Change default content of authenticators before VDA installation.
f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.
g. Document authenticator types approved for use, the frequency for changing/refreshing them, and the technical justification that demonstrates that this frequency provides adequate security.
h. Protect authenticator content from unauthorized disclosure and modification.
i. Require individuals to take, and to have devices implement, specific security safeguards to protect authenticators.

j. Change authenticators for group/role accounts when membership to those accounts changes.

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

E-34 Password-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (1))

For password-based authentication for the VDA, [Licensee/Applicant] does the following:

a. Enforce a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security.
b. Enforce password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters.
c. Enforce a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries.
d. Store and transmit only cryptographically protected passwords.
e. Enforce lifetime restrictions for password minimums of 1 day and provide a technical basis for maximums defined and documented by the CST that prevents unauthorized access.
f. Prohibit password reuse for 10 generations.
g. Require an immediate change to a permanent password upon the first logon when temporary passwords are used for VDA logons.
h. Store written or electronic copies of master passwords in a secure location with limited access.

E-35 Public Key Infrastructure-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (2))

[Licensee/Applicant] ensures that public key infrastructure-based authentication for the VDA does the following:

a. validates certifications by constructing and verifying a certification path to an accepted trust anchor and by checking certificate status information,
b. enforces authorized access to the corresponding private key,
c. maps the authenticated identity to the account of the individual or group, and
d. implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information through the network.

E-36 Hardware Token-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (11))

[Licensee/Applicant] ensures that the VDA for hardware token-based authentication uses 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, Revision 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, Revision 4, IA-7)

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

E-39 Incident Response Training
(Informed by NIST SP 800-53, Revision 4, IR-2, IR-2 (1), and IR-2 (2))

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

a. within 92 days of assuming an incident response role or responsibility,
b. when required by VDA changes, and
c. at least every 12 months.

[Licensee/Applicant] does the following:

a. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
b. Use automated mechanisms to provide a more thorough and realistic incident response training environment.

E-40 Incident Response Testing
(Informed by NIST SP 800-53, Revision 4, IR-3 and IR-3 (2))

[Licensee/Applicant] does the following:

a. Test 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 document the results of checklists, walkthrough or tabletop exercises, and simulations (parallel/full interrupt).
b. Test the incident response capability for the VDA at least every 36 months using a comprehensive exercise.
c. Coordinate incident response testing with organizational elements responsible for related plans.

E-41 Incident Handling
(Informed by NIST SP 800-53, Revision 4, IR-4, IR-4 (1), and IR-4 (4))

[Licensee/Applicant] does the following:

a. Implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
b. Coordinate incident-handling activities with contingency planning activities.
c. Incorporate lessons learned from ongoing incident-handling activities into incident response procedures, training, and testing and implement the resulting changes accordingly.
d. Use automated mechanisms to support the incident-handling process.
e. Correlate 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, Revision 4, IR-5 and IR-5 (1))

[Licensee/Applicant] does the following:

a. Track and document VDA security incidents.

b. Use 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, Revision 4, IR-6 and IR-6 (1))

[Licensee/Applicant] does the following:

a. Require personnel to report suspected cyber security incidents to the CST upon discovery.
b. Use automated mechanisms to assist in the reporting of security incidents.

E-44 Incident Response Assistance
(Informed by NIST SP 800-53, Revision 4, IR-7, IR-7 (1), and IR-7 (2))

[Licensee/Applicant] does the following:

a. Provide 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.
b. Use automated mechanisms to increase the availability of incident response-related information and support.

[Licensee/Applicant] does the following:

a. Establish a direct, cooperative relationship between its incident response capability and external providers of cyber security protection capabilities.
b. Identify organizational cyber security incident response team members to the external providers.

E-45 Controlled Maintenance
(Informed by NIST SP 800-53, Revision 4, MA-2 and MA-2 (2))

[Licensee/Applicant] does the following:

a. Perform and document maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern.
b. Review records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days.
c. Approve and monitor all maintenance activities whether these activities are performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.
d. Require the CST to approve the removal of the VDA for offsite maintenance or repairs outside the licensee's positive control.
e. Sanitize equipment to remove all information from associated media before removal for offsite maintenance or repairs outside the licensee's positive control.
f. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
g. Include in records of maintenance and repairs on VDA components, at a minimum, the date, time, identification of those performing the maintenance, description of maintenance performed, and list of VDA components removed or replaced.
h. Retain records for inspection by the NRC.
i. Use automated mechanisms to schedule, conduct, and document maintenance and repairs.
j. Produce 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, Revision 4, MA-3, MA-3 (1), and MA-3 (2))

[Licensee/Applicant] does the following:

a. Approve, control, and monitor VDA maintenance tools.
b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
c. Check 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 doing the following:

a. verifying that there is no VDA information contained on the equipment,
b. sanitizing or destroying the equipment,
c. retaining the equipment within the facility, or
d. 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, Revision 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant] does the following:

a. Approve and monitor nonlocal maintenance and diagnostic activities.
b. Document and only allow 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).
c. Use strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.
d. Maintain records for nonlocal maintenance and diagnostic activities.
e. Terminate session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant] does one of the following:

a. Document the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
b. Remove the component to be serviced from the VDA before using nonlocal maintenance or diagnostic services; sanitize the component (with regard to VDA information) before removing it from licensee facilities; and, after the service is performed, inspect and sanitize the component (with regard to potentially malicious software) before reconnecting it to the VDA.

E-48 Maintenance Personnel
(Informed by NIST SP 800-53, Revision 4, MA-5 and MA-5 (1))

[Licensee/Applicant] does the following:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
b. Ensure that unescorted personnel performing maintenance on the VDA have the required access authorizations.
c. Designate 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] does the following:

a. Implement procedures for the use of maintenance personnel who lack appropriate security clearances that include the following requirements:
   (1) Approved personnel who are fully cleared, have appropriate access authorizations, and are technically qualified escort and supervise maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals during the performance of maintenance and diagnostic activities on the VDA.
   (2) Before 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.
b. Develop and implement alternate security safeguards in the event that a VDA component cannot be sanitized, removed, or disconnected from the VDA.

E-49 Timely Maintenance

(Informed by NIST SP 800-53, Revision 4, MA-6)

[Licensee/Applicant] obtains maintenance support or spare parts, or both, for VDAs that are required to remain operational to prevent a consequence of concern.

E-50 Media Access

(Informed by NIST SP 800-53, Revision 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media include any active storage device, passive storage device, or passive media that have one of the following characteristics:

a. They contain information used to manage, configure, maintain, secure, or operate the VDA.
b. They are used on the VDA for any purpose.

E-51 Media Marking

(Informed by NIST SP 800-53, Revision 4, MP-3)

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

E-52 Media Storage

(Informed by NIST SP 800-53, Revision 4, MP-4)

[Licensee/Applicant] does the following:

a. Physically control and securely store VDA media.
b. Protect 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, Revision 4, MP-5 and MP-5 (4))

[Licensee/Applicant] does the following:

a. Protect and control VDA media during transport outside of controlled areas.
b. Maintain accountability for VDA media during transport outside of controlled areas.
c. Document activities associated with the transport of VDA media.
d. Restrict the activities associated with the transport of VDA media to authorized personnel.

e. Implement 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, Revision 4, MP-6, MP-6 (1), MP-6 (2), and MP-6 (3))

[Licensee/Applicant] does the following:

a. Sanitize VDA media before disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary.
b. Review, approve, track, document, and verify media sanitization and disposal actions.
c. Use sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
d. Test sanitization equipment and procedures at least every 12 months to verify that the intended sanitization is being achieved.
e. Apply nondestructive sanitization techniques to portable storage devices before connecting such devices to the VDA.

E-55 Media Use
(Informed by NIST SP 800-53, Revision 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, Revision 4, PE-6)

[Licensee/Applicant] does the following:

a. Monitor physical access to the facility where the VDA resides to detect and respond to physical security incidents.
b. Review physical access logs in a timely manner and upon occurrence of anomalous behavior.
c. Coordinate results of reviews and investigations with the organizational incident response capability.

E-57 Vulnerability Scanning
(Informed by NIST SP 800-53, Revision 4, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), and RA-5 (5))

[Licensee/Applicant] does the following:

a. Scan for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA or applications, or both, are identified and reported.
b. Use vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards that require the following:
   (1) enumeration of platforms, software flaws, and improper configurations;
   (2) formatting of checklists and test procedures; and
   (3) measurement of vulnerability impact.
c. Analyze vulnerability scan reports and results from security control assessments.
d. Address vulnerabilities in a timely and technically justified manner to prevent a consequence of concern.

e. Share 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).
f. Use vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned.
g. Update the VDA vulnerabilities scanned before performing a new scan.
h. Use vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information VDA components scanned and vulnerabilities checked).
i. Determine what information about the VDA is discoverable by adversaries and take measures to address the associated potential cyber security issues.
j. Implement privileged access authorization to the VDA for vulnerability scanning activities.

E-58 External Information System Services
(Informed by NIST SP 800-53, Revision 4, SA-9 and SA-9 (2))

[Licensee/Applicant] does the following:
a. Require providers of external information system services that interact with VDAs to comply with information security requirements and to address security controls for the associated consequence of concern.
b. Define and document oversight and user roles and responsibilities with regard to external information system services.
c. Use automated mechanisms to monitor security control compliance by external service providers on an ongoing basis.
d. Require 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, Revision 4, SA-10)

[Licensee/Applicant] requires the developer of the VDA, component, or information system service to do the following:
a. Perform configuration management during the VDA, component, or service lifecycle.
b. Document, manage, and control the integrity of changes to the VDA, component, or service.
c. Implement only organization-approved changes to the VDA, component, or service.
d. Document approved changes to the VDA, component, or service and the potential security impacts of such changes.
e. Track security flaws and flaw resolution within the VDA, component, or service and report findings to the CST.

E-60 Developer Security Testing and Evaluation
(Informed by NIST SP 800-53, Revision 4, SA-11)

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

E-61 Development Process, Standards, and Tools
(Informed by NIST SP 800-53, Revision 4, SA-15)

[Licensee/Applicant] does the following:

a. Require the developer of the VDA, VDA component, or VDA service to follow a documented development process that does the following:
   (1) explicitly addresses security requirements,
   (2) identifies the standards and tools used in the development process, and
   (3) documents the specific tool options and tool configurations used in the development process.
b. Document, manage, and ensure the integrity of changes to the process or tools, or both, used in development.
c. Review the development process, standards, tools, and tool options/configurations to determine whether the process, standards, tools, and tool options/configurations selected and used can satisfy VDA security requirements.

E-62 Developer Security Architecture and Design
(Informed by NIST SP 800-53, Revision 4, SA-17)

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

a. is consistent with and supportive of the licensee's security architecture;
b. accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and
c. 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, Revision 4, SC-2, SC-3, and SC-4)

[Licensee/Applicant] does the following:

a. Separate user functionality on the VDA (including user interface services) from VDA management functionality.
b. Isolate security functions from nonsecurity functions on the VDA.
c. Prevent unauthorized and unintended information transfer via shared resources.

E-64 Denial of Service Protection
(Informed by NIST SP 800-53, Revision 4, SC-5)

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

E-65 Boundary Protection
(Informed by NIST SP 800-53, Revision 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] does the following:

a. Monitor and control communications at the boundary of the VDA and at key internal boundaries within the VDA.
b. Implement subnetworks for publicly or externally accessible VDA components that are physically or logically separated from internal [Licensee/Applicant] networks.

c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security architecture.
d. Limit the number of external network connections to the VDA.

E-66 Transmission Confidentiality and Integrity
(Informed by NIST SP 800-53, Revision 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures that the VDA does the following:
a. protects the confidentiality and integrity of transmitted information and
b. 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, Revision 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 that are necessary to prevent a consequence of concern.

E-68 Cryptographic Key Establishment and Management
(Informed by NIST SP 800-53, Revision 4, SC-12 and SC-12 (1))

[Licensee/Applicant] does the following:
a. Establish and manage cryptographic keys for required cryptography used within the VDA in accordance with the NIST Cryptographic Module Validation Program.
b. Maintain availability of information necessary to safely operate the VDA or to 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, Revision 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 that the VDA does the following:
a. prohibits remote activation of collaborative computing devices except where explicitly authorized,
b. provides an explicit indication of use to users physically present at the devices,
c. provides physical disconnect of collaborative computing devices in a manner that supports ease of use, and
d. provides an explicit indication of current participants in collaborative sessions.

E-70 Public Key Infrastructure Certificates
(Informed by NIST SP 800-53, Revision 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
(Informed by NIST SP 800-53, Revision 4, SC-19)

[Licensee/Applicant] does the following:

a. Establish usage restrictions and implementation guidance for VoIP technology based on its potential to cause damage to the VDA if it is used maliciously.
b. Authorize, monitor, and control the use of VoIP within the VDA.

E-72 Secure Name/Address Resolution
(Informed by NIST SP 800-53, Revision 4, SC-20, SC-20a, SC-21, and SC-22)

[Licensee/Applicant] ensures that the VDA does the following:

a. provides additional data origin authentication and integrity verification artifacts for the VDA along with the authoritative name resolution data that the VDA returns in response to external name/address resolution queries,
b. 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 such domains are operating as part of a distributed hierarchical namespace,
c. requests and performs data origin authentication and data integrity verification on the name/address resolution responses that the VDA receives from authoritative sources, and
d. collectively provides fault-tolerant name/address resolution service for an organization and implements internal/external role separation.

E-73 Session Authenticity
(Informed by NIST SP 800-53, Revision 4, SC-23)

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

E-74 Fail in Known State
(Informed by NIST SP 800-53, Revision 4, SC-24)

[Licensee/Applicant] does the following:

a. Ensure that VDAs fail in a known state to ensure that functions are not adversely impacted.
b. Prevent 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, Revision 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, Revision 4, SC-39)

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

E-77 Flaw Remediation
(Informed by NIST SP 800-53, Revision 4, SI-2, SI-2 (1) and SI-2 (2))

[Licensee/Applicant] does the following:

a. Identify, report, and correct VDA flaws.

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
c. Correct the flaw expeditiously using the configuration management process.
d. Incorporate flaw remediation into the organizational configuration management process.
e. Perform vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production.
f. Centrally manage the flaw remediation process.
g. Use 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, Revision 4, SI-3, SI-3 (1), SI-3 (2), SI-3 (8), and SI-2 (10))

[Licensee/Applicant] does the following:

a. Use malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code.
b. Update malicious code protection mechanisms whenever new releases are available.
c. Configure malicious code protection mechanisms to do the following:
   (1) Perform periodic scans of the VDA at least every 7 days.
   (2) Perform real-time scans of files from external sources as the files are downloaded, opened, or executed.
   (3) Prevent malicious code execution.
   (4) Alert the CST of the detection of malicious code in a timely manner.
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA.
e. Centrally manage malicious code protection mechanisms.
f. Automatically update malicious code protection mechanisms for the VDA.
g. Detect unauthorized operating system commands in VDAs through the kernel application programming interface and do the following:
   (1) Issue a warning.
   (2) Audit the command execution.
   (3) Prevent the execution of the command.
h. Use tools and techniques to analyze the characteristics and behavior of malicious code.
i. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

E-79 VDA Monitoring

(Informed by NIST SP 800-53, Revision 4, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-4 (10), SI-4 (11), and SI-4 (20))

[Licensee/Applicant] does the following:

a. Monitor the VDA to detect the following:
   (1) cyber attacks and indicators of potential cyber attacks and
   (2) unauthorized local, network, and remote connections.
b. Identify unauthorized use of the VDA using automated or other means.
c. Deploy monitoring devices as follows:
   (1) strategically within the VDA to collect organization-determined essential information and
   (2) at ad hoc locations within the system to track specific types of transactions of interest to the organization.
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Heighten 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.
f. Provide VDA monitoring information to appropriate licensee cyber security personnel as necessary.
g. Use automated tools to support near real-time analysis of events.
h. Monitor inbound and outbound communications traffic for the VDA in near real time for unusual or unauthorized activities or conditions.
i. Ensure appropriate cyber security personnel are notified when indications of compromise or potential compromise of the VDA occurs.
j. Make provisions so that encrypted communications traffic is visible to authorized network monitoring tools.
k. Analyze outbound communications traffic at the external boundary of the VDA and selected interior points within the VDA to discover anomalies.
l. Implement additional monitoring of privileged users.

E-80 Security Alerts, Advisories, and Directives
(Informed by NIST SP 800-53, Revision 4, SI-5 and SI-5 (1))

[Licensee/Applicant] does the following:
a. Receive security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis.
b. Generate internal security alerts, advisories, and directives as necessary to prevent a consequence of concern.
c. Disseminate security alerts, advisories, and directives to appropriate personnel and the NRC.
d. Implement security directives in a timely manner.
e. Use automated mechanisms to make security alert and advisory information available throughout the organization.

E-81 Security Function Verification
(Informed by NIST SP 800-53, Revision 4, SI-6 and SI-6 (3))

[Licensee/Applicant] does the following:
a. Verify the correct operation of security functions.
b. Perform this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and upon discovery of anomalies.
c. Notify 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, Revision 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] does the following:
a. Use integrity verification tools to detect unauthorized changes to VDA software, firmware, and information.
b. Perform an integrity check of VDA software, firmware, and information where possible upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and upon discovery of anomalies.

c. Use automated tools that provide notification to appropriate personnel upon discovering discrepancies during integrity verification.
d. Automatically take proactive protection measures when VDA integrity violations are discovered.
e. Incorporate the detection of unauthorized security-relevant changes to the VDA into the organizational incident response capability.
f. Require that the integrity of software be verified before execution.
g. Prohibit 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, Revision 4, SI-11)

[Licensee/Applicant] ensures that the VDA does the following:
a. generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries and
b. 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, Revision 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, Revision 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, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, issued April 2013, AC-2)

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

a. Assign account managers for VDA accounts.
b. Establish conditions for group and role membership.
c. Specify authorized users of the VDA, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
d. Require independent management approval for requests to create VDA accounts.
e. Create, enable, modify, disable, and remove VDA accounts in accordance with the access control policy.
f. Monitor the use of VDA accounts.
g. Notify account managers in a timely manner of the following:
   (1) when accounts are no longer required,
   (2) when users are terminated or transferred, and
   (3) when individual VDA usage or need-to-know changes.
h. Authorize access to the VDA based on the following:
   (1) a valid access authorization, and
   (2) intended VDA usage.
i. Review accounts at least every 30 days for compliance with account management requirements.
j. Establish 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, Revision 4, AC-2 (5), AC-2 (12), and AC-2 (13))

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

a. Require that users log out within 15 minutes of inactivity unless the login session is required to be maintained to prevent a consequence of concern.
b. Monitor VDA accounts for atypical usage and anomalous activity that could indicate account compromise.
c. Report atypical usage of VDA accounts to the Cyber Security Team (CST).
d. Disable user accounts that have been potentially compromised upon discovery.

F-3 Automated Account Management
(Informed by NIST SP 800-53, Revision 4, AC-2 (1), AC-2 (2), AC-2 (3), and AC-2 (4))

To support the management of VDA accounts, [Licensee/Applicant] uses, at a minimum, automated technical mechanisms that do the following:

a. Automatically remove or disable temporary and emergency accounts once they are no longer needed.
b. Automatically disable inactive accounts within 30 days.
c. Automatically audit account creation, modification, enabling, disabling, and removal actions and notify appropriate personnel in a timely manner.

F-4 Access Management
(Informed by NIST SP 800-53, Revision 4, AC-3 and AC-4)

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

a. logical access to VDA information and VDA resources in accordance with applicable access control policies and
b. control of the flow of information within the VDA and between interconnected systems and VDAs.

F-5 Remote Access
(Informed by NIST SP 800-53, Revision 4, AC-17)

[Licensee/Applicant] does the following:

a. Establish and document usage restrictions, configurations, connection requirements, and implementation guidance for each type of remote access allowed.
b. Authorize remote access to the VDA before allowing such connections.

F-6 Managed Access Control Points
(Informed by NIST SP 800-53, Revision 4, AC-17 (3))

[Licensee/Applicant] ensures that all remote access to VDAs is through a boundary control device that meets the cyber security control requirements in "Boundary Control" of this appendix.

F-7 Wireless Access
(Informed by NIST SP 800-53. Revision 4, AC-18)

[Licensee/Applicant] does the following:

a. Establish usage restrictions, configurations, connection requirements, and implementation guidance for wireless access.
b. Authorize wireless access to the VDA before allowing such connections.

F-8 Restrict Configurations by Users
(Informed by NIST SP 800-53, Revision 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, Revision 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, Revision 4, AC-21)

When [Licensee/Applicant] shares VDA information with external parties, it does the following:

a. Ensure that access authorizations assigned to the sharing partner match the access restrictions on the information.
b. Use automated mechanisms to enforce these restrictions.

F-11 Use of External Information Systems
(Informed by NIST SP 800-53, Revision 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 do the following:

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

[Licensee/Applicant] does the following:

a. Restrict the use of organization-controlled portable storage devices by authorized individuals on external information systems.
b. Permit authorized individuals to use an external information system to access the VDA or to process, store, or transmit organization-controlled information only when [Licensee/Applicant] does the following:
   (1) verifies the implementation of security controls on the external system equivalent to security controls addressed for the VDA or
   (2) 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, Revision 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 that the VDA does the following:

a. 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
b. generates records containing information necessary to prevent a consequence of concern from a cyber attack, including, at a minimum, the following:
   (1) account (user or service) login failure;
   (2) account role or privilege change,
   (3) file or object creation, modification, and deletion;
   (4) service start and stop;
   (5) privileged service call;
   (6) account creation and modification;

(7) account right assignment;
(8) audit policy change;
(9) user account password change;
(10) user group creation and modification; and
(11) remote session start and failure.

[Licensee/Applicant] ensures that the VDA auditing function does the following:

a. alerts cyber security personnel in near real time of an audit processing failure or where audit failure events occur that could indicate VDA compromise,
b. takes automated measures to preserve audit data,
c. provides the capability to increase or modify audit record content in response to threat intelligence,
d. initiates session audits at VDA startup,
e. provides the capability for authorized users to select a user session to capture/record or view/hear,
f. provides the capability for authorized users to capture/record and log content related to a user session, and
g. 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, Revision 4, AU-4, AU-5 (1), AU-9 (2), AU-9 (3), AU-9 (4), and AU-10)

[Licensee/Applicant] does the following:

a. Allocate sufficient audit record storage capacity in accordance with U.S. Nuclear Regulatory Commission (NRC) record retention requirements and configure auditing to prevent exceedance of capacity.
b. Authorize access to management of audit functionality only to authorized users with cyber security responsibilities.

[Licensee/Applicant] ensures that the VDA does the following:

a. provides an alert to authorized personnel when allocated audit record storage volume reaches 80 percent of repository maximum audit record storage capacity;
b. backs up audit records onto a physically different system than the VDA or component being audited;
c. protects audit information and audit tools from unauthorized access, modification, and deletion;
d. implements cryptographic mechanisms to protect the integrity of audit information and audit tools; and
e. protects against an individual (or process acting on behalf of an individual) who falsely denies having performed any action on the VDA.

F-14 Audit Review, Analysis, and Reporting
(Informed by NIST SP 800-53, Revision 4, AU-6, AU-6a, AU-6b, AU-6 (1), and AU-6 (3))

[Licensee/Applicant] does the following:

a. Use automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
b. Review and analyze VDA audit records in a timely manner for indications of potential compromise.
c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
d. Report findings to the CST.

F-15 Independence of Assessors
(Informed by NIST SP 800-53, Revision 4, CA-2 (1), CA-7 (1), CA-8, and CA-8 (1))

[Licensee/Applicant] does the following:

a. Use 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.
b. Use 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.
c. Conduct penetration testing at least every 12 months on the VDA.
d. Use 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, Revision 4, CA-2 (2))

[Licensee/Applicant] includes and documents the following as part of VDA security control assessments:

a. an attack tree/attack surface analysis of the VDA (to be done at least every 24 months);
b. announced assessments that include the following:
   (1) in-depth monitoring (to be done automatically in real time),
   (2) vulnerability scanning (to be done at least every 30 days), and
   (3) malicious actor testing (to be done at least every 92 days); and
c. unannounced assessments (in addition to announced assessments above) that include the following:
   (1) vulnerability scanning (to be done at least every 183 days) and
   (2) malicious actor testing (to be done at least every 12 months).

F-17 Enhancements to VDA Connections
(Informed by NIST SP 800-53, Revision 4, CA-3 (3), CA-3 (4), CA-3 (5), and CA-9)

[Licensee/Applicant] does the following:

a. Use a "deny-all, permit-by-exception" policy for allowing VDAs to connect to external information systems.
b. Prohibit the direct connection of a VDA to an external network without the use of the following:
   (1) at least one separate, intervening access control device (e.g., firewall and cross-domain solution);
   (2) at least one separate, intervening intrusion detection/prevention mechanism with near real-time prevention, detection, and alerting capability;
   (3) host-based protective measures; and
   (4) other measures necessary to prevent a consequence of concern.
c. Prohibit the direct connection of a VDA to a public network.
d. Authorize connections to the VDA.
e. Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.

F-18 Configuration of VDAs for High-Risk Areas
(Informed by NIST SP 800-53, Revision 4, CM-2 (7))

[Licensee/Applicant] ensures that the CST does the following:

a. issues permission for individuals traveling with a VDA to locations that the [Licensee/Applicant] considers risks significant and
b. reviews the VDA upon return to ensure that the device is uncompromised.

F-19 Configuration Change Control
(Informed by NIST SP 800-53, Revision 4, CM-3)

[Licensee/Applicant] does the following:

a. Document changes to the VDA and provide configuration control in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.53, "Requirements for Cyber Security at Nuclear Fuel Cycle Facilities."
b. Review proposed configuration-controlled changes to the VDA and approve or disapprove such changes with explicit consideration for security impact analyses before implementation of the change.
c. Document configuration change decisions associated with the VDA.
d. Implement approved configuration-controlled changes to the VDA.
e. Retain records of configuration-controlled changes to the VDA in accordance with NRC record retention requirements.
f. Audit and review activities associated with configuration-controlled changes to the VDA.
g. Coordinate and provide oversight for configuration change control activities through the change management process.

F-20 Change Testing and Analysis
(Informed by NIST SP 800-53, Revision 4, CM-3 (2) and CM-4)

[Licensee/Applicant] does the following:

a. Test, validate, and document changes to the VDA before implementing the changes to the VDA.
b. Analyze changes to the VDA to determine potential security impacts before implementing the changes.

F-21 Access Restrictions for Change
(Informed by NIST SP 800-53, Revision 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, Revision 4, CM-6, CM-6 (1), and CM-6 (2))

[Licensee/Applicant] does the following:

a. Establish and document configuration settings within the VDA that reflect the most restrictive mode consistent with operational requirements.
b. Implement the configuration settings.
c. Identify, document, and approve any deviations from established configuration settings.
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
e. Use automated mechanisms to centrally manage, apply, and verify VDA configuration settings.

f. Report 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, Revision 4, CM-7)

[Licensee/Applicant] does the following:

a. Configure the VDA to provide only essential capabilities to perform its function and maintain safe and secure operations.
b. Prohibit or restrict the use of unneeded functions, ports, protocols, and/or services.

F-24 Periodic Review
(Informed by NIST SP 800-53, Revision 4, CM-7 (1))

[Licensee/Applicant] does the following:

a. Review the VDA at least every 30 days to identify unnecessary and/or nonsecure functions, ports, protocols, and services.
b. Disable or restrict unneeded functions, ports, protocols, and/or services identified by the review.

F-25 Authorized Software
(Informed by NIST SP 800-53, Revision 4, CM-7 (2) and CM-7 (4))

[Licensee/Applicant] does the following:

a. Identify software programs authorized to execute on the VDA.
b. Use a "deny-all, allow-by-exception" policy to prohibit the execution of unauthorized software programs on the VDA.
c. Review and update the list of authorized software programs at least every 183 days.
d. Use 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, Revision 4, CM-8, CM-8 (1), and CM-8 (3))

[Licensee/Applicant] does the following:

a. Develop and document an inventory of VDA components that does the following:
   (1) accurately reflects the current VDA,
   (2) includes all components within the boundary of the VDA,
   (3) is at the level of granularity necessary for tracking and reporting, and
   (4) includes information necessary to achieve effective VDA component accountability.
b. Review and update the VDA component inventory at least every 92 days or as part of any changes to a VDA.
c. Update the inventory of VDA components as an integral part of component installations, removals, and VDA updates.
d. Use automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the VDA.
e. Take 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, Revision 4, CM-11)

[Licensee/Applicant] does the following:

a. Establish policies governing the installation of software on VDAs consistent with the configuration management requirements in 10 CFR 73.53(f).
b. Enforce software installation policies using automated measures where supported.
c. Monitor policy compliance using automated measures where supported.

F-28 Identification and Authentication
(Informed by NIST SP 800-53, Revision 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 that the VDA does the following:

a. uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and nonorganizational users (or processes acting on behalf of nonorganizational users);
b. implements multifactor authentication for network access to privileged accounts;
c. implements multifactor authentication for network access to nonprivileged accounts;
d. implements multifactor authentication for local access to privileged accounts;
e. implements replay-resistant authentication mechanisms for network access to privileged accounts;
f. implements multifactor authentication for remote access to privileged and nonprivileged accounts such that a device separate from the system gaining access provides one of the factors and the device meets e-authentication assurance Level 3 as described in NIST SP 800-63-2, "Electronic Authentication Guideline," issued August 2013, or later revisions;
g. accepts and electronically verifies Personal Identity Verification credentials; and
h. uniquely identifies and authenticates devices before establishing a connection to a VDA.

F-29 Identifier Management
(Informed by NIST SP 800-53, Revision 4, IA-4)

[Licensee/Applicant] manages VDA identifiers by doing the following:

a. receiving independent management authorization to assign an individual, group, role, or device identifier;
b. selecting an identifier that identifies an individual, group, role, or device;
c. assigning the identifier to the intended individual, group, role, or device;
d. preventing reuse of identifiers where reuse could allow unintended or unauthorized access; and
e. disabling the identifier within 60 days of inactivity.

F-30 Authenticator Management
(Informed by NIST SP 800-53, Revision 4, IA-5)

[Licensee/Applicant] manages VDA authenticators by doing the following:

a. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. establishing initial authenticator content for authenticators defined by the organization;
c. ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. establishing and implementing administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revocation of authenticators;
e. changing default content of authenticators before VDA installation;

f. establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. documenting authenticator types approved for use, the frequency for changing/refreshing them, and the technical justification that demonstrates that this frequency provides adequate security;
h. protecting authenticator content from unauthorized disclosure and modification;
i. requiring individuals to take, and to have devices implement, specific security safeguards to protect authenticators; and
j. changing authenticators for group/role accounts when membership to those accounts changes.

F-31 Password-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (1))

For password-based authentication for the VDA, [Licensee/Applicant] does the following:
a. Enforce a minimum password length, strength, and complexity that is within the capabilities of the VDA and commensurate with the required level of security.
b. Enforce password complexity such that the passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters.
c. Enforce a sufficient number of changed characters when new passwords are created to ensure adversaries cannot determine the current password from previous entries.
d. Store and transmit only cryptographically protected passwords.
e. Enforce lifetime restrictions for password minimums of 1 day and provide a technical basis for maximums defined and documented by the CST that prevents unauthorized access.
f. Prohibit password reuse for 10 generations.
g. Require an immediate change to a permanent password upon the first logon when temporary passwords are used for VDA logons.

[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-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (2))

[Licensee/Applicant] ensures that public key infrastructure-based authentication for the VDA does the following:
a. validates certifications by constructing and verifying a certification path to an accepted trust anchor and by checking certificate status information,
b. enforces authorized access to the corresponding private key,
c. maps the authenticated identity to the account of the individual or group, and
d. implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

F-33 Hardware Token-Based Authentication
(Informed by NIST SP 800-53, Revision 4, IA-5 (11))

[Licensee/Applicant] ensures that hardware token-based authentication for the VDA uses 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, Revision 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.

F-35 Cryptographic Module Authentication
(Informed by NIST SP 800-53, Revision 4, IA-7)

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

F-36 Incident Response Training
(Informed by NIST SP 800-53, Revision 4, IR-2)

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

a. within 92 days of assuming an incident response role or responsibility,
b. when required by VDA changes, and
c. at least every 12 months.

F-37 Incident Response Testing
(Informed by NIST SP 800-53, Revision 4, IR-3 and IR-3 (2))

[Licensee/Applicant] does the following:

a. Test 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 document the results of checklists, walkthrough or tabletop exercises, and simulations (parallel/full interrupt).
b. Test the incident response capability for the VDA at least every 36 months using a comprehensive exercise.
c. Coordinate incident response testing with organizational elements responsible for related plans.

F-38 Incident Handling
(Informed by NIST SP 800-53, Revision 4, IR-4 and IR-4 (1))

[Licensee/Applicant] does the following:

a. Implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
b. Coordinate incident-handling activities with contingency planning activities.
c. Incorporate lessons learned from ongoing incident-handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
d. Use automated mechanisms to support the incident-handling process.

F-39 Incident Monitoring
(Informed by NIST SP 800-53, Revision 4, IR-5)

[Licensee/Applicant] tracks and documents VDA security incidents.

F-40 Incident Reporting
(Informed by NIST SP 800-53, Revision 4, IR-6 and IR-6 (1))

[Licensee/Applicant] does the following:

a. Require personnel to report suspected cyber security incidents to the CST upon discovery.
b. Use automated mechanisms to assist in the reporting of security incidents.

F-41 Incident Response Assistance
(Informed by NIST SP 800-53, Revision 4, IR-7 and IR-7 (1))

[Licensee/Applicant] does the following:

a. Provide 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.
b. Use automated mechanisms to increase the availability of incident response-related information and support.

F-42 Controlled Maintenance
(Informed by NIST SP 800-53, Revision 4, MA-2)

[Licensee/Applicant] does the following:

a. Perform and document maintenance and repairs on VDAs in a timely manner to prevent a consequence of concern.
b. Review records for maintenance and repairs on VDAs in accordance with manufacturer or vendor specifications but at least every 30 days.
c. Approve and monitor all maintenance activities whether these activities are performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.
d. Require the CST to approve the removal of the VDA for offsite maintenance or repairs outside the licensee's positive control.
e. Sanitize equipment to remove all information from associated media before removal for offsite maintenance or repairs outside the licensee's positive control.
f. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
g. Include in records of maintenance and repairs on VDA components, at a minimum, the date, time, identification of those performing the maintenance, description of maintenance performed, and list of VDA components removed or replaced.
h. Retain records for inspection by the NRC.

F-43 Maintenance Tools
(Informed by NIST SP 800-53, Revision 4, MA-3, MA-3 (1), and MA-3 (2))

[Licensee/Applicant] does the following:

a. Approve, control, and monitor VDA maintenance tools.
b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
c. Check 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, Revision 4, MA-4, MA-4 (2), and MA-4 (3))

[Licensee/Applicant] does the following:

a. Approve and monitor nonlocal maintenance and diagnostic activities.
b. Document and only allow 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).
c. Use strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.
d. Maintain records for nonlocal maintenance and diagnostic activities.
e. Terminate session and network connections when nonlocal maintenance is completed.

[Licensee/Applicant] does one of the following:

a. Document the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
b. Remove the component to be serviced from the VDA before using nonlocal maintenance or diagnostic services; sanitize the component (with regard to VDA information) before removing it from licensee facilities; and, after the service is performed, inspect and sanitize the component (with regard to potentially malicious software) before reconnecting it to the VDA.

F-45 Maintenance Personnel
(Informed by NIST SP 800-53, Revision 4, MA-5)

[Licensee/Applicant] does the following:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
b. Ensure that unescorted personnel performing maintenance on the VDA have the required access authorizations.
c. Designate 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, Revision 4, MA-6)

[Licensee/Applicant] obtains maintenance support or spare parts, or both, for VDAs that are required to remain operational to prevent a consequence of concern.

F-47 Media Access
(Informed by NIST SP 800-53, Revision 4, MP-2)

[Licensee/Applicant] restricts access to VDA media to authorized individuals only. VDA media include any active storage device, passive storage device, or passive media that have one of the following characteristics:

a. They contain information used to manage, configure, maintain, secure, or operate the VDA.
b. They are used on the VDA for any purpose.

F-48 Media Marking
(Informed by NIST SP 800-53, Revision 4, MP-3)

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

F-49 Media Storage
(Informed by NIST SP 800-53, Revision 4, MP-4)

[Licensee/Applicant] does the following:

a. Physically control and securely store VDA media.
b. Protect 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, Revision 4, MP-5 and MP-5 (4))

[Licensee/Applicant] does the following:

a. Protect and control VDA media during transport outside of controlled areas.
b. Maintain accountability for VDA media during transport outside of controlled areas.
c. Document activities associated with the transport of VDA media.
d. Restrict the activities associated with the transport of VDA media to authorized personnel.
e. Implement 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, Revision 4, MP-6)

[Licensee/Applicant] does the following:

a. Sanitize VDA media before disposal, release out of organizational control, or release for reuse in a manner that would prevent recovery of the data by an adversary.
b. Use 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, Revision 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, Revision 4, RA-5, RA-5 (1), RA-5 (2), and RA-5 (5))

[Licensee/Applicant] does the following:

a. Scan for vulnerabilities in the VDA and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the VDA or applications, or both, are identified and reported.
b. Use vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards that require the following:
   (1) enumeration of platforms, software flaws, and improper configurations;
   (2) formatting of checklists and test procedures; and

(3) measurement of vulnerability impact.

c. Analyze vulnerability scan reports and results from security control assessments.
d. Address vulnerabilities in a timely and technically justified manner to prevent a consequence of concern.
e. Share 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).
f. Use vulnerability scanning tools that include the capability to readily update the VDA vulnerabilities to be scanned.
g. Update the VDA vulnerabilities scanned before performing a new scan.
h. Implement privileged access authorization to the VDA for vulnerability scanning activities.

F-54 External Information System Services
(Informed by NIST SP 800-53, Revision 4, SA-9 and SA-9 (2))

[Licensee/Applicant] does the following:

a. Require the providers of external information system services that interact with VDAs to comply with information security requirements and to address security controls for the associated consequence of concern.
b. Define and document oversight and user roles and responsibilities with regard to external information system services.
c. Use automated mechanisms to monitor security control compliance by external service providers on an ongoing basis.
d. Require 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, Revision 4, SA-10)

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

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

F-56 Developer Security Testing and Evaluation
(Informed by NIST SP 800-53, Revision 4, SA-11)

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

a. Create and implement a security assessment plan.
b. Perform comprehensive cyber security testing and evaluation.
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
d. Implement a verifiable flaw remediation process.
e. Correct flaws identified during security testing and evaluation.

F-57 System Protection
(Informed by NIST SP 800-53, Revision 4, SC-2 and SC-4)

[Licensee/Applicant] does the following:

a. Separate user functionality of the VDA (including user interface services) from VDA management functionality.
b. Prevent unauthorized and unintended information transfer through shared resources.

F-58 Denial of Service Protection
(Informed by NIST SP 800-53, Revision 4, SC-5)

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

F-59 Boundary Protection
(Informed by NIST SP 800-53, Revision 4, SC-7, SC-7 (3), SC-7 (4), SC-7 (5), and SC-7 (7))

[Licensee/Applicant] ensures that the VDA does the following:

a. monitors and controls communications at the boundary of the VDA and at key internal boundaries within the VDA;
b. implements subnetworks for publicly or externally accessible VDA components that are physically or logically separated from internal [Licensee/Applicant] networks;
c. connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security architecture; and
d. denies network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny-all, permit-by-exception policy).

[Licensee/Applicant] limits the number of external network connections to the VDA.

F-60 External Telecommunications Services
(Informed by NIST SP 800-53, Revision 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] does the following:

a. Implement a managed interface for each external telecommunication service.
b. Establish a traffic-flow policy for each managed interface.
c. Protect the confidentiality and integrity of the information being transmitted across each interface.
d. Document each exception to the traffic-flow policy with a supporting mission/business need and duration of that need.
e. Review exceptions to the traffic-flow policy on a timely basis and remove exceptions that are no longer supported by an explicit mission/business need.
f. Prevent the unauthorized exfiltration of information across managed interfaces.
g. Allow only incoming communications from authorized sources to be routed to VDAs.
h. Implement host-based firewalls on VDAs.
i. Protect against unauthorized physical connections to the VDA.
j. Use boundary protection mechanisms.

[Licensee/Applicant] ensures that the VDA does the following:

a. has managed interfaces, denies network communications traffic by default, and allows network communications traffic by exception (i.e., deny-all, permit-by-exception policy);

b. prevents, in conjunction with a remote device, the device from simultaneously establishing nonremote connections with the system and communicating through some other connection to resources in external networks;
c. routes internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
d. provides the capability to dynamically isolate/segregate VDAs from other VDAs; and
e. 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, Revision 4, SC-8 and SC-8 (1))

[Licensee/Applicant] ensures that the VDA does the following:
a. protects the confidentiality and integrity of transmitted information and
b. 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, Revision 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 that are necessary to prevent a consequence of concern.

F-63 Cryptographic Key Establishment and Management
(Informed by NIST SP 800-53, Revision 4, SC-12 and SC-12 (1))

[Licensee/Applicant] does the following:
a. Establish and manage cryptographic keys for required cryptography used within the VDA in accordance with the NIST Cryptographic Module Validation Program.
b. Maintain availability of information necessary to safely operate the VDA or to 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, Revision 4, SC-15)

[Licensee/Applicant] ensures that the VDA does the following:
a. prohibits remote activation of collaborative computing devices except where explicitly authorized and
b. 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, Revision 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
(Informed by NIST SP 800-53, Revision 4, SC-19)

[Licensee/Applicant] does the following:

a. Establish usage restrictions and implementation guidance for voice over Internet protocol (VoIP) technology based on its potential to cause damage to the VDA if it is used maliciously.
b. Authorize, monitor, and control the use of VoIP within the VDA.

F-67 Secure Name/Address Resolution
(Informed by NIST SP 800-53, Revision 4, SC-20, SC-20a, SC-21, and SC-22)

[Licensee/Applicant] ensures that the VDA does the following:

a. provides additional data origin authentication and integrity verification artifacts for the VDA along with the authoritative name resolution data that the VDA returns in response to external name/address resolution queries,
b. 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 such domains are operating as part of a distributed hierarchical namespace,
c. requests and performs data origin authentication and data integrity verification on the name/address resolution responses that the VDA receives from authoritative sources, and
d. collectively provides fault-tolerant name/address resolution service for an organization and implements internal/external role separation.

F-68 Session Authenticity
(Informed by NIST SP 800-53, Revision 4, SC-23)

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

F-69 Protection of Information at Rest
(Informed by NIST SP 800-53, Revision 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, Revision 4, SC-39)

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

F-71 Flaw Remediation
(Informed by NIST SP 800-53, Revision 4, SI-2 and SI-2 (2))

[Licensee/Applicant] does the following:

a. Identify, report, and correct VDA flaws.
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
c. Correct the flaw expeditiously using the configuration management process.
d. Incorporate flaw remediation into the organizational configuration management process.
e. Perform vulnerability scans and assessments of the VDA to validate that the flaw has been eliminated before the VDA is put into production.
f. Use 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, Revision 4, SI-3, SI-3 (1), and SI-3 (2))

[Licensee/Applicant] does the following:

a. Use malicious code protection mechanisms at VDA network entry and exit points to detect and eradicate malicious code.
b. Update malicious code protection mechanisms whenever new releases are available.
c. Configure malicious code protection mechanisms to do the following:
   (1) Perform periodic scans of the VDA at least every 7 days.
   (2) Perform real-time scans of files from external sources as the files are downloaded, opened, or executed.
   (3) Prevent malicious code execution.
   (4) Alert the CST of the detection of malicious code in a timely manner.
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the VDA.
e. Centrally manage malicious code protection mechanisms.
f. Automatically update malicious code protection mechanisms for the VDA.

F-73 VDA Monitoring
(Informed by NIST SP 800-53, Revision 4, SI-4, SI-4 (2), SI-4 (4), and SI-4 (5))

[Licensee/Applicant] does the following:

a. Monitor the VDA to detect the following:
   (1) cyber attacks and indicators of potential cyber attacks and
   (2) unauthorized local, network, and remote connections.
b. Identify unauthorized use of the VDA using automated or other means.
c. Deploy monitoring devices as follows:
   (1) strategically within the VDA to collect organization-determined essential information and
   (2) at ad hoc locations within the system to track specific types of transactions of interest to the organization.
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
e. Heighten 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.
f. Provide VDA monitoring information to appropriate licensee cyber security personnel as necessary.
g. Use automated tools to support near real-time analysis of events.
h. Monitor inbound and outbound communications traffic for the VDA in near real time for unusual or unauthorized activities or conditions.
i. Ensure that the 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, Revision 4, SI-5)

[Licensee/Applicant] does the following:

a. Receive cyber security alerts, advisories, and directives from diverse and credible external sources on an ongoing basis.
b. Generate internal security alerts, advisories, and directives as necessary.

c. Disseminate security alerts, advisories, and directives to appropriate personnel and the NRC.
d. Implement security directives in a timely manner.

F-75 Security Function Verification
(Informed by NIST SP 800-53, Revision 4, SI-6 and SI-6 (3))

[Licensee/Applicant] does the following:
a. Verify the correct operation of security functions.
b. Perform this verification upon startup and restart, upon command by a user with appropriate privilege, at least every 7 days, and upon discovery of anomalies.
c. Notify appropriate personnel in a timely manner of failed security verification tests.
d. Report the results of security function verification to the CST.

F-76 Software, Firmware, and Information Integrity
(Informed by NIST SP 800-53, Revision 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] does the following:
a. Use integrity verification tools to detect unauthorized changes to VDA software, firmware, and information.
b. Perform an integrity check of VDA software, firmware, and information where possible upon startup and restart, upon command by a user with appropriate privilege, at least every 30 days, and upon discovery of anomalies.
c. Incorporate 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, Revision 4, SI-11)

[Licensee/Applicant] ensures that the VDA does the following:
a. generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries and
b. reveals error messages only to personnel responsible for VDA operation and maintenance.

F-78 Information Handling and Retention
(Informed by NIST SP 800-53, Revision 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.

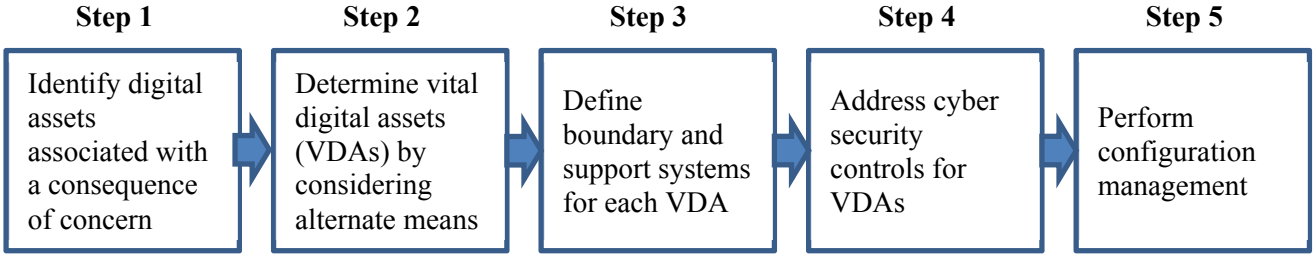
F-79 Memory Protection
(Informed by NIST SP 800-53, Revision 4, SI-16)

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

APPENDIX G

EXAMPLE IDENTIFICATION PROCESS, ALTERNATE MEANS ANALYSIS, IMPLEMENTING PROCEDURE, AND ADDITIONAL CONSIDERATIONS

For the purposes of this example, ACME, Inc. (ACME) is a fictitious, NRC licensed Category III fuel cycle facility (FCF) with two process lines. The licensee is implementing the provisions of 10 *Code of Federal Regulations* (CFR) 73.53 "Requirements for Cyber Security at Nuclear Fuel Cycle Facilities" for their licensed operations. They have received NRC approval of their cyber security plan and formed a Cyber Security Team. They are currently implementing their cyber security program and this example chronicles the process as outlined in the following diagram.



Step 1 – Identify Digital Assets Associated with a Consequence of Concern

ACME provided the following description of a generic process to identify digital assets in their approved cyber security plan.

> The facility's integrated safety analysis was used to inform the identification of all locations of chemicals and radiological materials having the potential to produce safety consequences of concern (i.e., radiological exposures of 0.25 Sv (25 rem) or greater for any individual, 30 milligrams or greater intakes of uranium in soluble form for any individual outside the controlled area, acute chemical exposures that could lead to irreversible or other serious long lasting health effects for any individual). The facility schematics and instrumentation diagrams, boundary packages for items relied on for safety (IROFS), network diagrams, and field walkdowns identify the digital assets performing safety functions for these locations. The licensee considers the safety functions of these devices, both at the component and system level, to determine if the functions could: (1) cause an active consequence of concern; or (2) prevent a latent consequence of concern.
>
> The facility's Standard Practices and Procedures Plan identifies all locations of classified information or matter. These locations are physically protected in accordance with 10 CFR Part 95. The facility schematics, instrumentation diagrams, network diagrams, and field walkdowns identify the digital assets performing security functions in these locations. ACME considers the security functions of these devices, both at the component and system level, to determine if the functions could prevent a latent security consequence of concern (i.e., loss or unauthorized disclosure of classified information or classified matter).
>
> ACME evaluates the digital assets identified above to develop a list of those whose functions, if compromised by a cyber attack, could result in a consequence of concern. This list provides: (1) the names and physical locations of the applications, devices,

systems, or networks identified as digital assets and (2) the types of consequences of concern applicable if the digital assets are compromised by a cyber attack.

ACME has committed in their cyber security plan to use the existing IROFS boundary packages as well as the engineering layout of the process lines to evaluate the digital assets' susceptibility to a consequence of concern due to a cyber attack. Based on this review, the digital assets associated with active and latent safety consequences of concern are identified.

ACME identifies three digital assets on process line 1:

a. Process control network for process line 1 – this is a collection of industrial control devices (e.g., motors, valves, and sensors) networked together with control panels and indicators to operate process line 1; and
b. Temperature control IROFS for process line 1 – these are temperature sensors that are isolated from the process control network and have the ability to shutdown process line 1 (i.e., safe state) under off-normal conditions; and
c. Pressure control IROFS for process line 1 – these are pressure sensors that are isolated from the process control network and have the ability to shutdown process line 1 (i.e., safe state) under off-normal conditions.

A release of the material in process line 1, due to high-temperature or over-pressurization, would cause an acute chemical exposure that could lead to irreversible or other serious long lasting health effects to a worker (i.e., consequence of concern). Compromise of the process control network could cause an active consequence of concern, while compromise of the temperature and pressure control IROFS could cause a latent consequence of concern.

ACME observes that all of the digital assets on process line 1 are air-gapped. Air-gapped digital assets are not physically connected to a network or to other digital systems.

ACME's second process line has analog controls but uses classified matter (e.g., information or equipment which is protected under 10 CFR Part 95). Process line 2 is in a closed section of the facility only accessible via a single entrance with a guard station. The physical security devices supporting the process line are reviewed to determine if any are associated with the latent security consequence of concern. Two digital assets were identified:

a. A surveillance system for process line 2 which consists of a collection of cameras and recorders connected to a local area network that is monitored by the guard station at the entrance to the area; and
b. A biometric reader that individuals use to gain access to process line 2 which consists of: (1) an electronic reader, at the entrance to the closed area; (2) a door sensor; and (3) door hardware.

A cyber attack on the digital assets identified for process line 2 could compromise a function needed to prevent loss or unauthorized disclosure of classified information or classified matter (i.e., latent security consequence of concern).

ACME documents the name, location, and associated consequence for each potential VDA in a list that is maintained on-site for NRC inspection:

Table G-1. ACME – (DRAFT) List of Digital Assets Associated with a Consequence of Concern, Alternate Means, and VDAs

Name	Location	Consequence of Concern	Alternate Means Present (yes or no)	Description of Alternate Means (if applicable)	Implementing Procedure # (applicable for VDAs)
Process line 1 control network	Process line 1	Active safety			
Temperature control IROFS	Process line 1	Latent safety			
Pressure control IROFS	Process line 1	Latent safety			
Process line 2 surveillance system	Process line 2	Latent security			
Process line 2 biometric reader	Process line 2	Latent security			

Step 2 – Determine VDAs by Considering Alternate Means

Further analysis of the identified digital assets is needed to determine if they are vital or if an alternate means exists to prevent a consequence of concern. ACME provided the following description in their approved cyber security plan for a generic process to analyze alternate means.

> The list of digital assets indicates the following: (1) whether an alternate means is relied on to prevent the specific consequence of concern and (2) a brief description of the alternate means, if applicable, for each digital asset. ACME credits only acceptable alternate means with the following attributes:
>
> a. Is available, reliable, and capable to perform the credited function(s);
> b. Is protected from a cyber attack;
> c. Is sufficiently reliable and adequately implemented consistent with other safety or security features;
> d. Is properly maintained and periodically tested;
> e. Prevents the identified consequence of concern;
> f. Would be implemented with available resources;
> g. would not be adversely impacted by the potential multi-node effects from a cyber attack;
> h. Considers the cumulative effects from a cyber attack; and
> i. Does not contribute to other cyber security vulnerabilities or lead to a consequence of concern.
>
> ACME credits an alternate means that is shared among multiple digital assets only if it is an acceptable alternate means and considers the potential cumulative effects from simultaneous compromise of the associated digital assets.
>
> ACME credits a manual action as an acceptable alternate means only after determining that the action is reliable. Detection of a compromise is not relied upon to initiate a manual action (i.e., reactive actions are not acceptable alternate means). ACME credits only reliable preventative manual actions after considering the following attributes:

a. Environmental factors (e.g., lighting, radiation levels, and temperature) that could affect the action;
b. Functionality and accessibility of necessary equipment to perform the action;
c. Indication and confirmation the action has the expected result;
d. Procedures and training for the action;
e. Adequate staffing to perform the action; and
f. Demonstration (e.g., testing) of the action.

ACME reviews the list of digital assets for process line 1 and evaluates potential alternate means for those assets. ACME's Table G-1 identifies three digital assets associated with a consequence of concern (i.e., process line 1 control network, temperature control IROFS, and pressure control IROFS). There are no alternate means (i.e., IROFS or otherwise) to prevent these consequence of concern, so ACME considers the temperature control IROFS and the pressure control IROFS as VDAs.

However, because the temperature and pressure control IROFS are VDAs, ACME decides to credit them as an alternate means for the process line 1 control network. A compromise of the process line 1 control network would not result in a consequence of concern because the temperature and pressure control IROFS prevent a release of material from occurring. ACME uses the alternate means analysis described in the cyber security plan to confirm that the temperature and pressure control IROFS are an acceptable alternate means of protection. With the presence of an acceptable alternate means, the process line 1 control network is not considered a VDA and is therefore not required to implement additional cyber security measures. The list of digital assets is notated accordingly, see ACME's revised list in Table G-2 below.

ACME reviews the list of digital assets for process line 2. ACME's draft list in Table G-1 identifies two digital assets associated with a consequence of concern (i.e., process line 2 surveillance system and biometric reader). They examine whether there is an alternate means to prevent the consequence of concern for those assets. ACME identifies that a guard force routinely patrols the area covered by the surveillance system. By using the commitments in their cyber security plan to evaluate the guard force, ACME determines that the guards are an acceptable alternate means to prevent the consequence of concern (i.e., latent – security) for the surveillance system.

However, the existing procedure used by the guard force only requires a visual check of badges in the event of a malfunctioning biometric reader. ACME's analysis determines that a cyber attack's compromise of the biometric reader may be undetectable. Therefore, ACME revises their Standard Practices and Procedures Plan and associated operating procedures to require that a guard confirms identification against a current, approved access control list before allowing entry. Furthermore, ACME confirms that there are sufficient guards to simultaneously perform the routine patrols and confirm identification, thereby preventing any cumulative effects from the compromise of both the process line 2 surveillance system and biometric reader. Therefore, ACME credits the guard force as an alternate means to prevent a latent-security consequence of concern. The list of digital assets is notated accordingly in ACME's revised list in Table G-2 below.

Table G-2. ACME – (REVISED) List of Digital Assets Associated with a Consequence of Concern, Alternate Means, and VDAs

Name	Location	Consequence of Concern	Alternate Means Present (yes or no)	Description of Alternate Means (if applicable)	Implementing Procedure # (applicable for VDAs)
Process line 1 control network	Process line 1	Active safety	Yes	Temperature control IROFS and pressure control IROFS	
Temperature control IROFS	Process line 1	Latent safety	No		
Pressure control IROFS	Process line 1	Latent safety	No		
Process line 2 surveillance system	Process line 2	Latent security	Yes	Guard force	
Process line 2 biometric reader	Process line 2	Latent security	Yes	Guard force	

Step 3 – Define Boundary and Support Systems for Each VDA

ACME identifies that compromise of either IROFS could independently cause a consequence of concern, therefore, as VDAs, the two IROFS for process line 1 each require protection from a cyber attack. ACME identifies the applicable cyber security controls from their cyber security plan to protect against the latent consequences of concern. By addressing the performance specifications of these controls, ACME puts measures in place to protect both IROFS. While each IROFS performs a different function, their designs are similar (a control panel connected to collection of sensors that are calibrated by a milliamp simulator). ACME takes advantage of type accreditation to group these VDAs and write one implementing procedure to cover both (e.g., Cy-1234). The implementing procedure is referenced for convenience in ACME's final list in Table G-3. For completeness, ACME references the system user manuals and information sheets detailing the components and network layout in the implementing procedure.

Table G-3. ACME – (FINAL) List of Digital Assets Associated with a Consequence of Concern, Alternate Means, and VDAs

Name	Location	Consequence of Concern	Alternate Means Present (yes or no)	Description of Alternate Means (if applicable)	Implementing Procedure # (applicable for VDAs)
Process line 1 control network	Process line 1	Active safety	Yes	Temperature control IROFS and pressure control IROFS	
Temperature control IROFS	Process line 1	Latent safety	No		Cy-1234
Pressure control IROFS	Process line 1	Latent safety	No		Cy-1234
Process line 2 surveillance system	Process line 2	Latent security	Yes	Guard force	
Process line 2 biometric reader	Process line 2	Latent security	Yes	Guard force	

ACME also analyzed the associated support systems and determined that the compromise of either power, environmental control, or both, could not cause or contribute to a consequence of concern with these VDAs. However, these IROFS do use a milliamp simulator (there are two total) for calibration. The milliamp simulators have no external connection capabilities, but mis-calibration of the VDAs by the milliamp simulators could cause a consequence of concern. Therefore, ACME includes them as a component within the VDA boundary. ACME uses a single implementing procedure addresses the cyber security controls applicable to a latent – safety consequence of concern for both VDAs and the milliamp simulators. An example implementing procedure and an excerpt of the controls with the corresponding measures taken, is provided below in the Temperature and Pressure Control IROFS – Cyber Security VDA Implementing Procedure (Cy-1234).

Step 4 – Address Cyber Security Controls for VDAs

The following is an example implementing procedure developed by ACME for their VDAs (temperature and pressure control IROFS). Included within the implementing procedure is an excerpt of the controls with the corresponding measures taken.

Temperature and Pressure Control IROFS – Cyber Security VDA Implementing Procedure (Cy-1234)

a. Network Diagram Reference and Physical Location for the VDA
   (1) See network operations guide (e.g., document #4567) for the network layout, and
   (2) VDAs affected by this procedure are found only on process line 1.

b. Identification of the VDA and Boundary
   (1) Temperature or pressure control IROFS, and
   (2) the boundary is the same as the temperature and pressure control IROFS boundary packages found in the ISA (document #7890).

c. Type(s) of Consequence of Concern
Latent – safety

d. Function, General Description, and Purpose of the VDA
These are temperature or pressure sensor systems on process line 1 that have the ability to override control of the line and shutdown should values approach safety thresholds. They are a collection of sensors along the process line for a given condition (i.e., temperature or pressure) that are directly linked to a control panel. The control panel can be configured directly and the sensors are calibrated using a milliamp simulator.

e. Individual(s) or Organization Responsible for the VDA
For the temperature or pressure control IROFS, the following parties are responsible for the various components:
(1) sensors and wiring (Facility Engineering Department),
(2) control panel (Information Technology (IT) Department), and
(3) milliamp simulator (IT Department).

f. Location, Interconnections, and Environment
(1) This VDA is located on process line 1 with a notification signal sent to the control room,
(2) it has no interconnections to other VDAs or systems, and
(3) it has no specific environmental requirements.

g. Support Systems for the VDA
No support systems were identified whose compromise could:
(1) provide an input to the VDAs that causes a consequence of concern;
(2) directly cause a consequence of concern; or
(3) preclude the VDAs from performing the function needed to prevent a consequence of concern.

h. Tools for the VDA
(1) Temperature or pressure control IROFS use common hand tools for maintenance;
(2) the milliamp simulator calibration uses no special software;
(3) each control panel configuration is done using onboard diagnostic and configuration routines.

i. Inventory (Hardware, Software, and Versions)
Information for the VDA can be found in the Process Line System Inventory (document #6198).

j. Standards and Applicable Cyber Security Controls
Provided in Table G-4 below.

Table G-4. Cy-1234 – Excerpt of Measures to Address Cyber Security Controls Performance Specifications

Control Name	Description of Measure
B-1 – Detection	Authorized personnel monitors logs and IROFS functionality in conjunction with the Temperature and Pressure Control IROFS Operating Procedures (e.g., documents #3356 and #3357).
B-8 – Privileged Accounts	Accounts for administration are setup in alignment with the Authorized Access List (e.g., document #7890) for Process Line 1 using the appropriate configuration guide.
B-14 – Log Events	Logging is properly established on each control panel using the appropriate configuration guide (e.g., document #987).
B-17 – VDA Connections	The attack pathway for this control does not exist. Given that the VDA does not connect to, and is incapable of connecting to, other digital assets, criterion B-17(a) is not applicable. Criterion B-17(b) is also not applicable as there are no interconnections to document. Criterion B-17(c) is not applicable as there are no authorizations to review.
F-2 – Account Management	Local accounts are to be properly established on each control panel using the appropriate configuration guide or system instruction.
F-5 – Remote Access	The attack pathway for this control does not exist. Given that the VDA is incapable of allowing remote access, criterion F-5(a) is not applicable. Criterion F-5(b) is also not applicable as there are no methods of remote access available to authorize.
F-46 – Timely Maintenance	Inherited from the Temperature and Pressure Control IROFS Maintenance Procedures (e.g., documents #4356 and #4357).
F-47 – Media Access	The attack pathway for this control does not exist. Given that the VDA does not connect to, and is incapable of connecting to, other digital assets, this is not applicable

k. Verification of Cyber Security Controls
ACME verifies the effectiveness of the measures taken to address the performance characteristics of each cyber security control by routinely testing access to the VDAs by attempting to use unauthorized credentials, reviewing the event logs, and maintaining the referenced procedures.

l. Temporary Compensatory Measures
Any measure not working is logged in ACME's facility maintenance log and a temporary compensatory measure is put in place, in accordance with the ACME Cyber Security Plan and monitored to completion.

Step 5 – Perform Configuration Management

Changes to digital assets (e.g., additions, modifications, or removal of devices and equipment) are evaluated by the ACME Cyber Security Team before their implementation and are confirmed to have no adverse impact on ACME's ability to meet the cyber security program objectives. ACME has documented this system in written procedures and has incorporated cyber security configuration management to their existing, site-wide configuration management program.

ACME evaluates additions or changes using a cyber security impact analysis. The ACME cyber security impact analysis for changes to the facility is conducted in accordance with Section C.9.1 of NRC's regulatory guide, "Cyber Security Programs for Nuclear Fuel Cycle Facilities."

ACME utilizes a VDA authorization process for the cyber security program. The VDA authorization process is performed in accordance with Section C.9.2 of NRC's regulatory guide, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," and is incorporated in the procedures for the configuration management system.

Additional Considerations

Based on the guidance provided in Section C.6.2 of NRC's regulatory guide, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," the temperature and pressure control IROFS in this example may have different considerations if a laptop was used for calibration or configuration. A laptop is traditionally not considered an air-gapped digital asset. During typical operations, a laptop requires some form of connectivity to apply updates, install software, or load data. That connectivity is considered before stating the associated digital asset is air-gapped, establishing the boundary for a VDA, and addressing the performance specifications of the applicable cyber security controls.

Also, based on the guidance provided in Section C.6.2 of NRC's regulatory guide, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," the temperature and pressure control IROFS in this example would have different considerations if they were connected to a network but behind a data diode. For instance, a VDA that is behind a data diode may state that control F-5, Remote Access, is addressed. For this example, a licensee could say:

> The attack pathway for this control does not exist. The VDA is prevented from receiving remote access connections due to its placement behind the data diode. Therefore, criterion F-5(a) is not applicable. Criterion F-5(b) is also not applicable as there are no interconnections to document. Criterion F-5(c) is not applicable as there are no authorizations to review.

However, if the VDA is capable of receiving communications of any kind from digital systems – including the data diode itself, as it may have some native communications capability, rather than simply being a passive device – ACME would not credit the data diode as satisfying the requirements of control B-17, VDA connections.

The use of a data diode may allow ACME to partially address the requirements of cyber security controls concerned with network-based attack paths. For example, in Control F-17, enhancements to VDA connections, criterion F-17(a) of this control is designed to be a policy statement or documented standard to apply to all VDAs. Criterion F-17(a) would only be addressed by a data diode if all VDAs were behind the data diode. For this example, a licensee could say:

a. The attack pathway for this control does not exist.

b. All VDAs are physically incapable of connecting to an external information network. This is enforced by the hardware disabling/removal of all non-Ethernet communications capability. Ethernet communications to VDAs from non-plant systems is prevented through the use of a data diode. Therefore, criterion F-17(a) is not applicable.

c. Criteria F-17(b) and F-17(c) are not applicable as there is no direct connection to external or public systems or networks. The data diode prevents any communication upstream through other means.

d. Criteria F-17(d) and F-17(e) are not applicable as there are no connections to external or public systems or networks to authorize or document.