NEI 13-10 [Revision 0]

Cyber Security Control Assessments

October 2013

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

NEI 13-10 [Revision 0]

Nuclear Energy Institute

Cyber Security Control Assessments

October 2013

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

ACKNOWLEDGMENTS

This document has been prepared by the nuclear power industry with input and guidance from the United States Nuclear Regulatory Commission. While many individuals contributed heavily to this document, NEI would like to acknowledge the significant leadership and contribution of the following individuals.

Executive sponsor:
James Meister Exelon Corporation

Core project team:
Patrick Asendorf Tennessee Valley Authority
William Gross Nuclear Energy Institute
Christopher Kelley Exelon Corporation
Jay Phelps South Texas Project Nuclear Operating Company

The core project team was supported by:
Nathan Faith Exelon Corporation
Jan Geib South Carolina Electric & Gas Company
James Shank PSEG Services Corporation
Laura Snyder Tennessee Valley Authority

Industry review team:
Glen Frix Duke Energy Corporation
Geoff Schwartz Entergy

NOTICE

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

EXECUTIVE SUMMARY

When the methodology to address cyber security controls was developed in the template for the cyber security plan, the industry believed there would be small handfuls of digital assets (CDAs) that would require a cyber security assessment. However, NEI understands that plants, including those with no digital safety-related systems, have identified many hundreds if not thousands of CDAs. Included are assets that range from those directly related to operational safety and security to those that, if compromised, would have no direct impact on operational safety, security, or emergency response capabilities. This guidance document was developed to minimize the burden on licensees to comply with their NRC approved cyber security plan, while continuing to ensure that the adequate protection criteria of 10 CFR 73.54 are met by streamlining the process to address cyber security controls for CDAs.

This document implements a graded, consequence-based approach to the implementation of cyber security controls for CDAs. This guidance document streamlines the process for addressing the cyber security controls referenced in the cyber security plan for large numbers of CDAs. Many CDAs in these plants have very limited technological capabilities. Combined with existing measures that are in place, the likelihood that an adversary could successfully compromise and exploit these CDAs to challenge operational safety, security, or emergency response capabilities is acceptably low.

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

TABLE OF CONTENTS

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

CYBER SECURITY CONTROL ASSESSMENTS

1 INTRODUCTION

1.1 BACKGROUND

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

10 CFR 73.54 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan.

Further, 10 CFR 50.34(c)(2) states in part that "Each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54 of this chapter." The Cyber Security Plan establishes the licensing basis for the Cyber Security Program.

The purpose of the Cyber Security Plan (CSP) is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented. The intent of the CSP is to protect the health and safety of the public from radiological sabotage as a result of a cyber attack. 10 CFR 50.34(c), "Physical Security Plan," requires the inclusion of a Physical Security Plan.

Section 3.1.6 of the CSP describes how licensees address cyber security controls for digital assets that have been identified for protection against cyber attacks. NEI 13-10 provides guidance licensees may use to address cyber security controls for CDAs consistent with the methodology described in CSP Section 3.1.6.

1.2 SCOPE

This document provides guidance licensees may use to address cyber security controls for those digital assets that a site specific analysis, performed in accordance with the requirements of 10 CFR 73.54 (b)(1), determined require protection from cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

1.3 PURPOSE

The purpose of this document is to provide guidance licensees may use to address cyber security controls for CDAs consistent with the methodology described in Section 3.1.6 of the Cyber Security Plan.

2 USE OF THIS DOCUMENT

The following method may optimize the use of the guidance in this document:

a) PRINT this document, particularly the body and Appendix A.

b) GATHER CDA-related information documented when implementing CSP Sections 3.1.3, 3.1.4, and 3.1.6.

c) PERFORM a consequence assessment of CDAs using the guidance in Section 3 of this document.

   i) USE the guidance in Sections 3, 4, and 5 of this document to determine if further cyber security control assessments are warranted for the CDAs.

d) USE the guidance in Section 6 to address cyber security controls for CDAs that the assessment performed using the guidance in Section 3 of this document determined require further cyber security control assessment.

e) DOCUMENT the assessment and RETAIN the documents in accordance with the CSP.

3 CONSEQUENCE ASSESSMENT OF CDAS

Licensees may use the guidance detailed in Table 1, "Consequence Assessment," to determine which of the approaches described in this document may be used to address cyber security controls for CDAs. Table 1 is illustrated in Figure 1, which can be found in Appendix A to this document. It is intended that any CDA subject to this assessment would proceed to one of the two exit states illustrated in Figure 1.

The Consequence Assessment provides a method to assess alternate means of performing EP functions, including offsite communications. The methodology of assessing alternate means is described in Section 4, "Function Maintained through Alternate Means." Where alternate means would ensure that sufficient defense-in-depth exists to mitigate the consequences of a cyber attack, additional cyber security controls would not be necessary. The alternate means provides defense-in-depth equivalent to the cyber security protections afforded by the cyber security controls.

The Consequence Assessment also provides guidance for determining if baseline cyber security protections provide adequate protection from cyber attacks for certain CDAs. The baseline cyber security controls are described in Section 5, "Baseline Cyber Security Protection Criteria." For these CDAs, the protection afforded by the implementation of the seven interim milestones and existing nuclear programs and processes provides high assurance that these CDAs are adequately protected against cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

A cyber security control assessment would be performed for CDAs that the Consequence Assessment determines would, if compromised, adversely impact equipment relied on for safety, security, or to respond to a radiological emergency. Section 6, "Considerations when Implementing Cyber Security Controls" provides guidance on addressing cyber security controls to ensure CDAs are adequately protected from cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

Figure 1 Question	Guidance
1.1	Would a compromise of the CDA result in a system level SSEP functional failure (i.e., adverse impact to system function, rather than to component function)? If YES, proceed to question 1.3 of this table. If NO, proceed to question 1.2 of this table. The definition of Adverse Impact (as documented in RG 5.71) includes the following: In the case where the direct or indirect compromise of a support system causes a safety, important to safety, security or emergency preparedness system or support system to actuate or "fail safe" and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds), this is not considered to be an adverse impact as it defined by 10 CFR 73.54(a). Criteria for answering 'NO': 1) Compromise of CDA would not result in system level SSEP functional failure (i.e., system remains capable performing its intended SSEP function); 2) A compromise of a CDA that provides indication only would not be a System level functional failure. 3) Compromise of CDA associated with SR/ITS functions: a) Would not result in the inability to implement emergency operating procedures; b) Would not result in entry to a condition requiring a plant trip within 15 minutes; or c) Equivalent system function impact could be accomplished via non-digital means (i.e. opening a breaker or closing a valve).
1.2	Are the baseline cyber security controls described in Section 5 of this document in place for the CDA? If YES, then current cyber security controls are adequate to meet CSP Section 3.1.6. If NO, enhance cyber security measures to meet the baseline cyber security controls described in Section 5 of this document.

Figure 1 Question	Guidance
1.3	Is the CDA in the Balance-of-Plant (BOP)? If YES, proceed to question 1.4 of this table. If NO, proceed to question 1.5 of this table. Consider referring to SSC scoping per 10 CFR 50.65(b)(2)(iii) for additional information regarding SSCs who's CDAs should be considered.
1.4	Would the compromise of the CDA initiate, or cause to be initiated, an automatic reactor or turbine trip, Engineered Safety Features Actuation (ESFA), or require shutdown in less than 24 hours? If YES, address cyber security controls for the CDA using the guidance in Section 6 of this document. If NO, proceed to question 1.2 of this table. Consider referring to SSC scoping per 10 CFR 50.65(b)(2)(iii) for additional information regarding SSCs who's CDAs should be considered.
1.5	Is the CDA associated with EP functions, including offsite communications, or are EP support systems or equipment for EP-related CDAs? If YES, proceed to question 1.6 of this table. If NO, address cyber security controls for the CDA using the guidance in Section 6 of this document.
1.6	Has an assessment using the process described in Section 4 and illustrated in Figure 2 determined that the EP functions are maintained through alternate means? If YES, then current cyber security controls are adequate to meet CSP Section 3.1.6. If NO, address cyber security controls for the CDA using the guidance in Section 6 of this document.

Table 1, Consequence Assessment

4 FUNCTION MAINTAINED THROUGH ALTERNATE MEANS

Licensees may use the guidance in Table 2, "Alternative Means Assessment," to determine if the functions of the assets that could be adversely impacted by a cyber attack can be maintained through alternate means. Table 2 is illustrated in Figure 2, which can be found in Appendix A to this document.

The guidance in Table 2 can be used to determine whether at least the minimum required set of equipment remains operable to perform the intended emergency response function despite a cyber attack. Where an assessment using the guidance in Table 2 determines that a cyber attack would not adversely impact the ability to implement the function, additional cyber security controls would not be warranted.

Changes to measures credited as providing an alternate method of maintaining the function should be subject to review (e.g., existing program reviews, procedure revision reviews, or use of configuration management) to ensure the changes would not challenge the adequacy of the alternate method.

Figure 2 Question	Guidance
2.1	Are alternate means available for performing the intended EP function, including offsite communications? If YES, proceed to question 2.2 of this table. If NO, protect CDA using guidance in Section 6 of this document.
2.2	Is one or more of the alternate means administrative, non-digital, or technologically diverse? If YES, proceed to question 2.3 of this table. If NO, proceed to question 2.6 of this table. Two means would be considered technologically diverse if they rely on substantially different technologies (e.g., a commercial computer system vs. an embedded device, or, a PBX-based phone system vs. satellite phones, etc.). Administrative methods, including actions performed by personnel, can be considered as an alternate means.
2.3	Is the alternate means documented? If YES, proceed to question 2.4 of this table. If NO, document the alternate means and then proceed to question 2.4 of this table. The means must be documented in a plan, policy, or implementing procedure.

Figure 2 Question	Guidance
2.4	Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? If YES, proceed to question 2.5 of this table. If NO, implement detection and response measures and then proceed to question 2.5 of this table. Measures for detection and response may be technical, procedural, or administrative, and could include periodic functional or availability testing (e.g., existing periodic operability tests performed on plant systems or equipment). The measures in place to must be performed at a frequency to ensure the ability to employ the alternate means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack. In certain cases, requirements exist regarding the duration that equipment could be unavailable. These requirements must be considered when determining the answer to question 2.4.
2.5	Are appropriate facility personnel trained to use the alternate method? If YES, then the function is maintained through alternate means. End assessment here. If NO, perform training of appropriate facility personnel. Once initiated, the function is maintained through alternate means. End assessment here.
2.6	If there a requirement to maintain a minimum set of equipment available, is the minimum required set of equipment adequately protected? If YES, then the function is maintained through alternate means. End assessment here. If NO, then at least the minimum required set of equipment should be protected using the guidance in Section 6 of this document. Requirements to maintain a minimum set of equipment may be found in Technical Specifications, system design documents, licensing documents, or implementing guidance.

Table 2, Alternative Means Assessment

5 BASELINE CYBER SECURITY PROTECTION CRITERIA

An assessment using the guidance in Section 3 permits licensees to credit baseline cyber security controls for CDAs that, if compromised, would not have a direct adverse impact on SSEP functions. For these CDAs, if baseline cyber security protections are in place, no further cyber security controls would be necessary. Specifically, for these CDAs, the baseline cyber security protections provide high assurance that CDAs are adequately protected against cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

Where a licensee chooses to credit these baseline cyber security controls for a CDA, the licensee should confirm these baseline controls are met.

A CDA may be considered to be adequately protected from cyber attacks if all of the following baseline cyber security criteria are met:

a) CDA is located within a Protected or Vital area;

b) CDA and any interconnected assets do not use wireless internetworking communications technologies;

c) CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device;

d) Use of portable media and mobile devices is controlled; and,

e) The CDA, or the equipment that would be affected by the compromise of the CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity should be consistent with timeframes identified in existing requirements, technical specifications, or other implementing guidance. The periodicity should be sufficient to allow a response prior to an adverse impact that would result from a cyber attack.

Where these baseline cyber security criteria are not met, the licensee may document and implement additional cyber security controls to ensure the baseline cyber security controls are met for the CDA.

Where these baseline cyber security criteria are met, additional cyber security controls are not necessary. Changes to the baseline cyber security controls should be subject to review to ensure CDAs remain adequately protected from cyber attacks.

6 CONSIDERATIONS WHEN IMPLEMENTING CYBER SECURITY CONTROLS

The following sections provide guidance that may be considered when addressing cyber security controls for CDAs and other devices requiring protection in accordance with licensee Cyber Security Plans (CSPs).

Licensees must use the approach documented in CSP Section 3.1.6 to address cyber security controls for CDAs. CSP Section 3.1.6 allows licensees to: implement the cyber security controls; implement alternative controls/countermeasures; or, not implement the cyber security controls. Alternative controls/countermeasures must eliminate the threat/attack vector(s) associated with the cyber security controls. The controls need not be implemented if the vulnerability or weakness it addresses does not exist, cannot be exploited, or if the attack vector it blocks or monitors does not exist.

The decision for which of the three approaches specified in Section 3.1.6 to use when addressing the security controls is dependent on many factors, including whether the device is isolated, part of an isolated (e.g. air-gapped) network or a device connected to one or more other networks. Licensees may use the information collected during tabletop review and validation activities performed in accordance with CSP Section 3.1.5 to determine if the device in question meets the definitions below for Type 1, Type 2, or Type 3 devices. Where a CDA meets these definitions, the guidance in these sections may be used to address cyber security controls for the CDA.

Appendix B, "Technical Cyber Security Control Applicability Matrices," of this document provides a documented consideration of each of the technical cyber security controls for Type 1, Type 2, and Type 3 devices. The particular focus of the this Section is to provide a streamlined approach for addressing cyber security controls for Type 1 and Type 2 devices. As demonstrated in the tables in Appendix B, for these categories of devices most technical cyber security controls are either not applicable based on the limited capabilities of these types of devices, or the control is implemented by an alternate countermeasure that mitigates the attack vector to the CDA.

The tables in Appendix B identify certain cyber security controls for Type 1 and Type 2 devices that must be addressed by licensees. The guidance in Section 6.4, "Technical Controls Assessment," provides a simplified method to identify and addressing these remaining cyber security controls.

6.1 TYPE 1 DEVICES

A Type 1 device is defined as a stand-alone component that is not network-connected with any other device(s). An isolated device may have networking capability, but to ensure it remains isolated, the networking capability should be disabled to the extent practical and controlled via approved configuration control practices.

Type 1 devices are simple digital components with a small attack surface that require physical access to alter or manipulate. In order to meet the definition for a Type 1 device the CDA in question should meet all of the following criteria:

a) No logical access (e.g. no user or administrative accounts or account management capability);

b) Does not support SYSLOG or comparable logging capability;

c) Disabled or no digital communications capability;

d) No ability to support identification or authentication; and,

e) Does not natively support malware protection or host-based intrusion detection.

As described more fully in Section 6.4, "Technical Cyber Security Control Assessment," for Type 1 devices, licensees should ensure the device is located within a Protected Area or has adequate physical access controls, and portable media controls are addressed to maintain high assurance that Type 1 CDAs are adequately protected from cyber attacks. Examples of typical Type 1 devices may include transmitters, indicators, and embedded firmware-based devices (e.g. field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), complex programmable logic devices (CPLDs), etc.).

6.2 TYPE 2 DEVICES

A Type 2 device is defined as a component that utilizes networking capability to communicate with other devices within a system that shares a common function. To be isolated, Type 2 devices must be part of an isolated or air-gapped network and cannot be connected to another device or network that serves a different system function. Changes to the networking functionality of Type 2 devices should be controlled via approved configuration control practices.

Type 2 devices are components with networking capability but a limited attack surface that requires physical access to alter or manipulate. In order to meet the definition for a Type 2 device the CDA in question should meet all of the following criteria:

a) Has limited logical access (e.g. generally only a user and/or administrative account);

b) Does not support SYSLOG or comparable logging capability;

c) Communications capability restricted to devices that share a common system function;

d) Identification and/or authentication limited to isolated network; and,

e) Does not natively support malware protection or host-based intrusion detection.

As described more fully in Section 6.4, "Technical Cyber Security Control Assessment," for Type 2 devices, licensees should ensure the device and interconnected devices are located within a Protected Area or has adequate physical access controls, portable media controls are addressed, logical access controls are addressed, and wired and wireless networking controls are addressed to maintain high assurance that Type 2 CDAs are adequately protected from cyber attacks. Examples of typical Type 2 devices may include programmable logic controllers, recorders, and devices that communicate via typical industrial communications protocols within an isolated network such as Fieldbus and Modbus.

6.3 TYPE 3 DEVICES

A Type 3 device is defined as a component that is part of a network connected to one or more other devices or networks with different functions. Type 3 devices are typically connected to other networks for the purposes of exchanging data. The connectivity of Type 3 devices is typically managed by a security boundary device(s) (e.g., data diodes, firewalls, etc.) that implements information flow enforcement controls. Changes to the networking functionality of Type 3 devices should be controlled in accordance with the licensee's Cyber Security Plan defensive strategy and approved configuration control practices. For Type 3 devices licensees should address the cyber security controls in accordance with CSP Section 3.1.6 to establish and maintain high assurance networked devices are adequately protected from cyber attacks. Examples of typical licensee Type 3 devices may include higher functioning devices such as client workstations, servers, network switches, and routers that use Ethernet and IP-based communications.

Devices such as the Security Computer host server serve different security functions, and therefore should be treated as a Type 3 device.

6.4 TECHNICAL CYBER SECURITY CONTROL ASSESSMENT

Table 3, "Technical Controls Assessment," provides guidance that may be used to address cyber security controls for CDAs that meet the criteria for Type 1, Type 2, or Type 3 CDAs as describe in Sections 5.1, 5.2 or 5.3 of this document, respectively. Table 3, "Technical Controls Assessment," is illustrated in Figure 3.

ID	Guidance
3.1	Can the CDA be defined as a Type 1 device using the criteria in Section 6.1 of this document? If YES, proceed to question 3.2 of this table. If NO, proceed to question 3.4 of this table.

ID	Guidance
3.2	Is the device located within a Protected Area or is physical access to the device adequately controlled? Adequate physical access control for devices outside the protected area may be achieved by addressing the Physical and Operational Environment Protection (E5) family of cyber security controls. If YES, proceed to question 3.3 of this table. If NO, remediate as required to achieve adequate physical access controls and proceed to question 3.3 of this table.
3.3	Are portable media access controls addressed? Portable media controls may be addressed by implementing the D1.19 technical cyber security control or implementing a portable media and mobile device program that addresses the D1.19 control. If YES, current measures are adequate to meet CSP Section 3.1.6. If NO, remediate as required to achieve address portable media access.
3.4	Can the CDA be defined as a Type 2 device using the criteria in Section 6.2 of this document? If YES, proceed to question 3.5 of this table. If NO, proceed to CSP Section 3.1.6 to address cyber security controls for the CDA.
3.5	Is the device located within a Protected Area or is physical access to the device adequately controlled? Adequate physical access is control for devices outside the protected area may be achieved by addressing the Physical and Operational Environment Protection (E5) family of cyber security controls. If YES, proceed to question 3.6 of this table. If NO, remediate as required to achieve adequate physical access controls and proceed to question 3.6 of this table.
3.6	Are portable media access controls addressed? Portable media controls may be addressed by implementing the D1.19 technical cyber security control or implementing a portable media and mobile device program that addresses the D1.19 control. If YES, proceed to question 3.7 of this table. If NO, remediate as required to achieve address portable media access and proceed to question 3.7 of this table.

ID	Guidance
3.7	Are logical access controls applied? Logical access controls should be addressed based on the capability and functionality of the device and at a minimum should address the following cyber security controls: D1.2, "Account Management;" D4.2 "User Identification and Authentication;" and, D4.3 "Password Requirements." If YES, proceed to question 3.8 of this table. If NO, remediate as required to achieve adequate logical access controls and proceed to question 3.8 of this table.
3.8	Are wired and wireless networking controls applied? Wired and wireless access controls should be addressed based on the capability and functionality of the device and at a minimum should address the following cyber security controls: D1.15, "Network Access Control;" and, D1.17, "Wireless Access Restrictions." If YES, current measures are adequate to meet CSP Section 3.1.6. If NO, remediate as required to achieve adequate wired and wireless networking access.

Table 3, Technical Controls Assessment

APPENDIX A – FIGURES

Appendix A provides figures illustrating the guidance in Sections 3, 4, and 6 of this document.

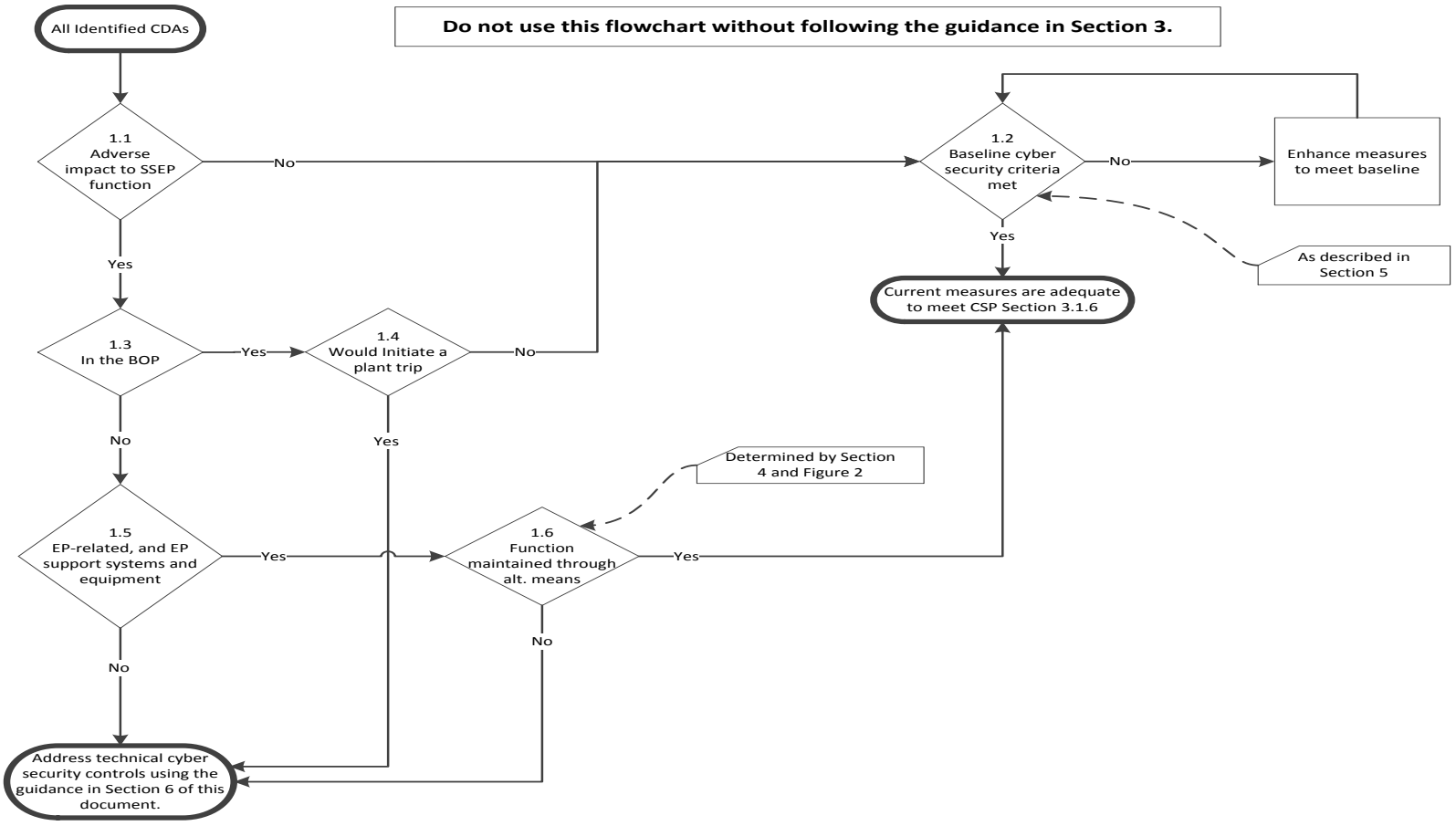

Figure 1 – Consequence Assessment

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

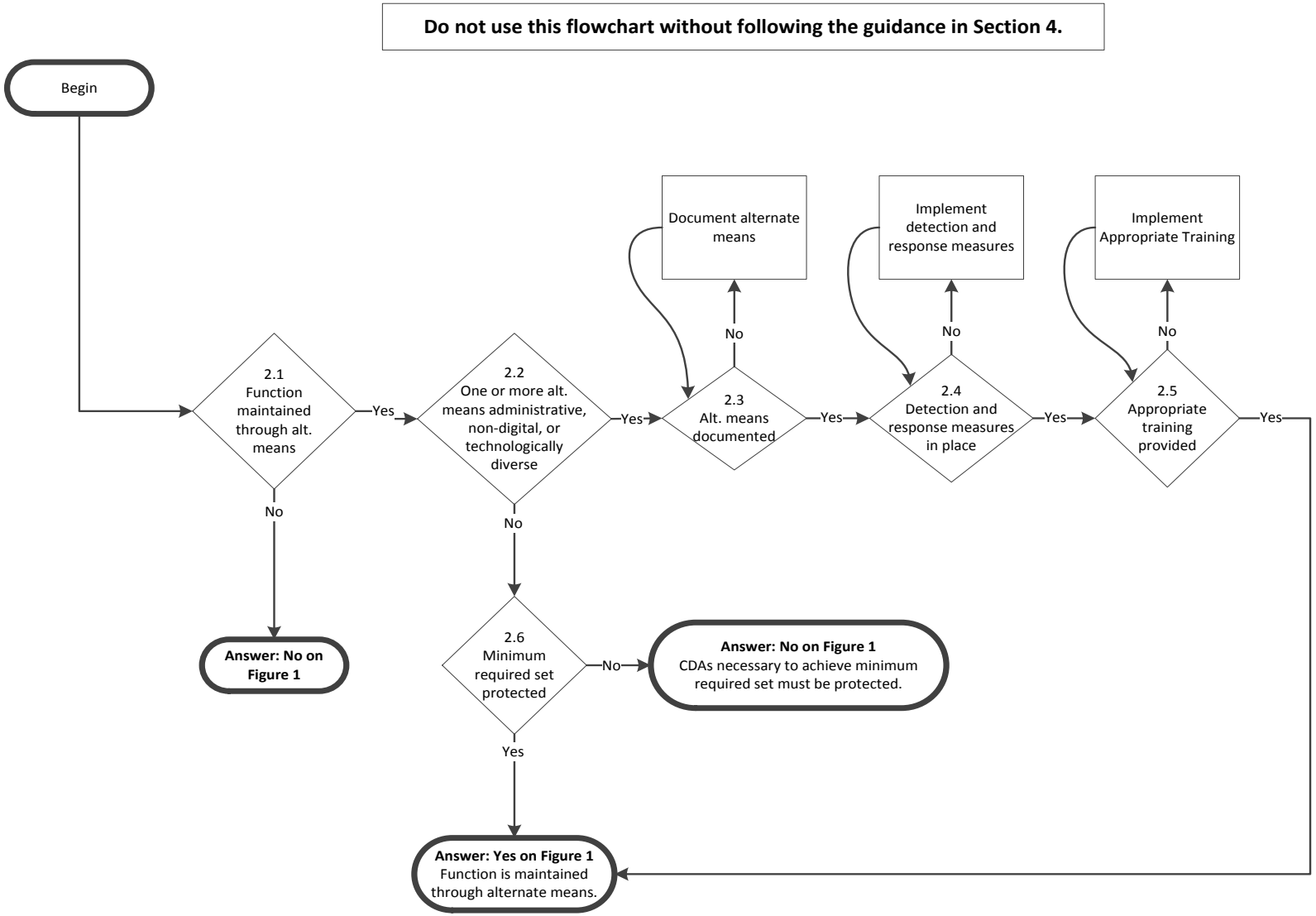

Figure 2 – Alternative Means Assessment

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

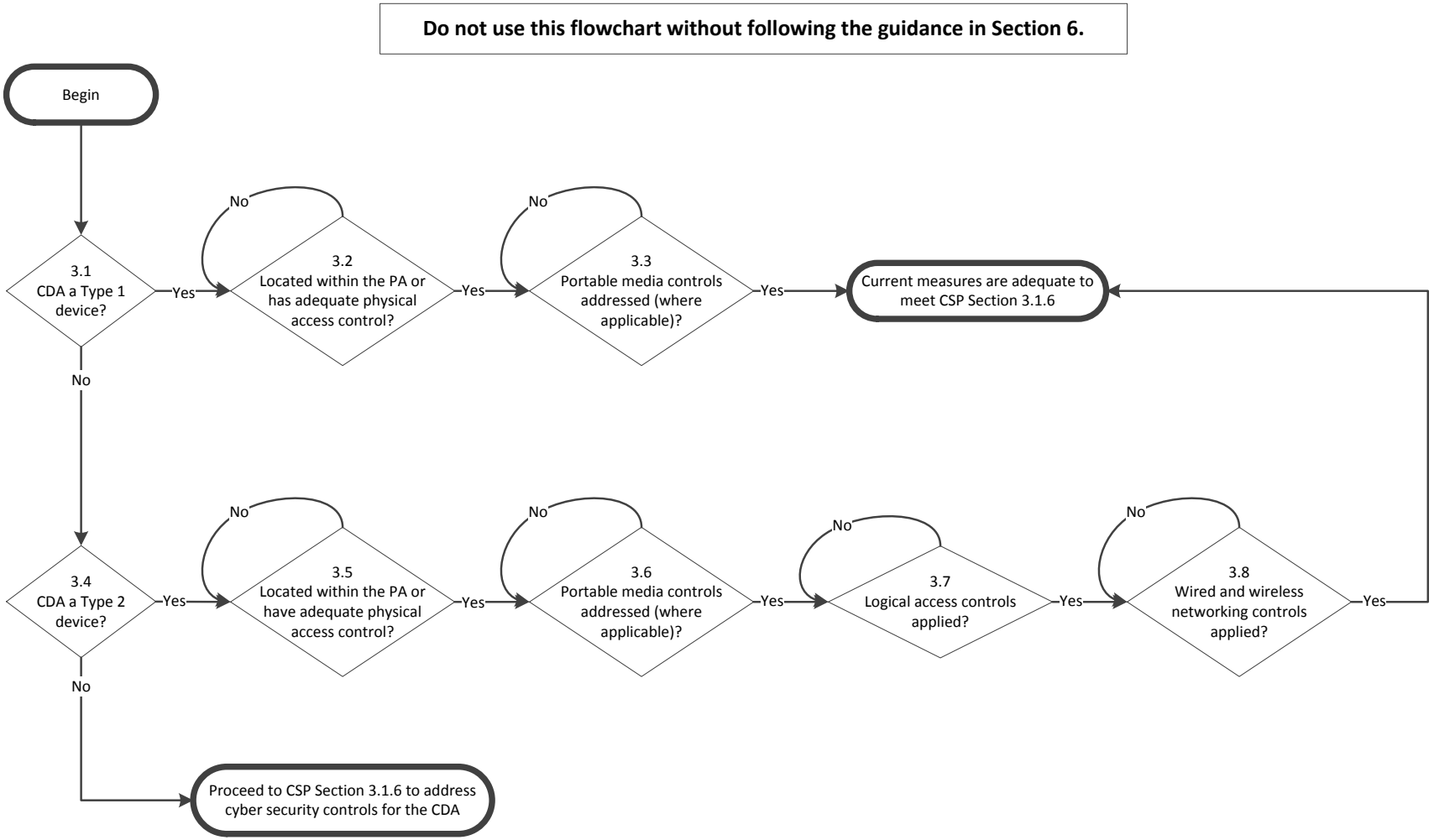

Figure 3 – Technical Cyber Security Controls Assessment

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX B – TECHNICAL CYBER SECURITY CONTROL APPLICABILITY MATRICES

Tables 1 through 5 of this Appendix provide a documented consideration of each of the technical cyber security controls for Type 1, Type 2, and Type 3 devices. The determinations documented in the tables in this Appendix are informed by the attributes of Type 1, Type 2, and Type 3 devices based on the criteria described in Sections 6.1, 6.2 and 6.3 of this document. The determinations are also informed by the cyber security protections implemented in the seven interim milestones and existing nuclear programs, including the Physical Protection Program. Controls labeled with an "M" are addressed and the attack vectors adequately mitigated by these existing security measures. No further action is required to address those cyber security controls.

CYBER SECURITY CONTROLS APPLICABILITY MATRIX	Legend A = Address the control M = Mitigated		
Typical Device Platforms	Type 1 Device	Type 2 Device	Type 3 Device
TECHNICAL CONTROLS			
ACCESS CONTROL FAMILY			
Account Management (D1.2)	M	A	A
Access Enforcement (D1.3)	M	M	A
Information Flow Enforcement (D1.4)	A	A	A
Separation of Functions (D1.5)	M	M	A
Least Privilege (D1.6)	M	M	A
Unsuccessful Logon Attempts (D1.7)	M	M	A
System Use Notification (D1.8)	M	M	A
Previous Logon Notification (D1.9)	M	M	A
Session Lock (D1.10)	M	M	A
Supervision and Review - Access Control (D1.11)	M	M	A
Permitted Actions without Identification or Authentication (D1.12)	M	M	A
Automated Marking (D1.13)	M	M	A
Automated Labeling (D1.14)	M	M	A
Network Access Control (D1.15)	M	A	A
“Open/Insecure” Protocol Restrictions (D1.16)	M	M	A
Wireless Access Restrictions (D1.17)	M	A	A
Insecure and Rogue Connections (D1.18)	M	M	A
Access Control for Portable and Mobile Devices (D1.19)	A	A	A
Proprietary Protocol Visibility (D1.20)	M	M	A
Third Party Products and Controls (D1.21)	M	M	A
Use of External Systems (D1.22)	M	M	A
Publicly Accessible Content (D1.23)	M	M	A

Table 1: Access Control Family Applicability Matrix

CYBER SECURITY CONTROLS APPLICABILITY MATRIX	Legend A = Address the control M = Mitigated		
Typical Device Platforms	Type 1 Device	Type 2 Device	Type 3 Device
TECHNICAL CONTROLS			
AUDIT AND ACCOUNTABILITY FAMILY			
Auditable Events (D2.2)	M	M	A
Content of Audit Records (D2.3)	M	M	A
Audit Storage Capacity (D2.4)	M	M	A
Response to Audit Processing Failures (D2.5)	M	M	A
Audit Review, Analysis, and Reporting (D2.6)	M	M	A
Audit Reduction and Report Generation (D2.7)	M	M	A
Time Stamps (D2.8)	M	M	A
Protection of Audit Information (D2.9)	M	M	A
Nonrepudiation (D2.10)	M	M	A
Audit Record Retention (D2.11)	M	M	A
Audit Generation (D2.12)	M	M	A

Table 2: Audit and Accountability Controls Applicability Matrix

CYBER SECURITY CONTROLS APPLICABILITY MATRIX	Legend A = Address the control M = Mitigated		
Typical Device Platforms	Type 1 Device	Type 2 Device	Type 3 Device
TECHNICAL CONTROLS			
SYSTEM AND COMMUNICATIONS PROTECTION FAMILY			
Application Partitioning and Security Function Isolation (D3.2)	M	M	A
Shared Resources (D3.3)	M	M	A
Denial of Service Protection (D3.4)	M	M	A
Resource Priority (D3.5)	M	M	A
Transmission Integrity (D3.6)	M	M	A
Transmission Confidentiality (D3.7)	M	M	A
Trusted Path (D3.8)	M	M	A
Cryptographic Key Establishment and Management (D3.9)	M	M	A
Unauthorized Remote Activation of Services (D3.10)	M	M	A
Transmission of Security Parameters (D3.11)	M	M	A
Public Key Infrastructure Certificates (D3.12)	M	M	A
Mobile Code (D3.13)	M	M	A
Secure Name/Address Resolution Service (Authoritative/Trusted Source) (D3.14)	M	M	A
Secure Name/Address Resolution Service (Recursive or Caching Resolver) (D3.15)	M	M	A
Architecture and Provisioning for Name/Address Resolution Service (D3.16)	M	M	A
Session Authenticity (D3.17)	M	M	A
Thin Nodes (D3.18)	M	M	A
Confidentiality of Information at Rest (D3.19)	M	M	A
Heterogeneity/Diversity (D3.20)	M	M	A
Fail in Known State (D3.21)	M	M	A

Table 3: System and Communications Protection Controls Applicability Matrix

CYBER SECURITY CONTROLS APPLICABILITY MATRIX	Legend A = Address the control M = Mitigated		
Typical Device Platforms	Type 1 Device	Type 2 Device	Type 3 Device
TECHNICAL CONTROLS			
IDENTIFICATION & AUTHENTICATION FAMILY			
User Identification and Authentication (D4.2)	M	A	A
Password Requirements (D4.3)	M	A	A
Non-authenticated Human Machine Interaction Security (D4.4)	M	M	A
Device Identification and Authentication (D4.5)	M	M	A
Identifier Management (D4.6)	M	M	A
Authenticator Management (D4.7)	M	M	A
Authenticator Feedback (D4.7)	M	M	A
Cryptographic Module Authentication (D4.9)	M	M	A

Table 4: Identification and Authentication Controls Applicability Matrix

CYBER SECURITY CONTROLS APPLICABILITY MATRIX	Legend A = Address the control M = Mitigated		
Typical Device Platforms	Type 1 Device	Type 2 Device	Type 3 Device
TECHNICAL CONTROLS			
SYSTEM HARDENING AND SELECT E3 FAMILY			
Removal of Unnecessary Services and Programs (D5.1)	M	M	A
Host Intrusion Detection System (D5.2)	M	M	A
Changes to File Systems and Operating Systems Permissions (D5.3)	M	M	A
Hardware Configuration (D5.4)	M	M	A
Installing Operating Systems, Applications and Third-Party Software Updates (D5.5)	M	M	A
Malicious Code Protection (E3.3)	M	M	A
Monitoring Tools and Techniques (E3.4)	M	M	A

Table 5: System Hardening Controls Applicability Matrix