Addendum 1 to NEI 08-09, Revision 6 Dated April 2010 Change Descriptions and Justifications

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.

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6 dated April 2010, provides a template for the implementation of the cyber security plan.

Lessons learned through licensee implementation efforts, and through a series of implementation workshops conducted during 2016 that included industry and NRC observers indicate that clarifications to NEI 08-09 are necessary. The changes are needed to enhance clarity and consistency in implementation, and to support NRC oversight activities.

The changes in this Addendum are consistent with the cyber security program performance objective to provide high assurance that digital computer and communications systems and networks are adequately protected against the design basis threat of radiological sabotage cyber attack as described in 10 CFR 73.1. The changes in this Addendum are intended to add necessary clarity without decreasing the effectiveness of cyber security plans implemented using the guidance in NEI 08-09.

1.2 PURPOSE

This addendum provides clarifications to NEI 08-09, Revision 6 to enhance clarity and consistency in implementation, and to support NRC oversight activities.

1.3 SCOPE

The guidance in this addendum is applicable to power reactor licensees with Cyber Security Plans (CSP) based on the template in NEI 08-09, Revision 6.

Section 2 provides a table of changes. Section 3 provides a description and a justification for each change, demonstrating that the change does not decrease the effectiveness of the CSP. Section 4 provides a 'red-line/strike-out' to the applicable sections in NEI 08-09, Revision 6. Section 5 provides the final text with changes incorporated.

1.4 USE OF THIS DOCUMENT

Licensees may incorporate the changes identified in this Addendum in accordance with the requirements of 10 CFR 50.54(p). While these changes do not constitute a decrease in the effectiveness of CSPs based on the guidance in NEI 08-09, Revision 6, licensees seeking to implement the changes in this Addendum must review the change(s) against their NRC approved CSP to confirm that those changes do not decrease the safeguards effectiveness of the CSP.

1.5 ACRONYMS

The following acronyms are used in this document:

CAP – Corrective Action Program
CDA – Critical Digital Asset
CSP – Cyber Security Plan
DAS – Data Acquisition System
EP – Emergency Preparedness
GPS - -Global Positioning System
LLEA – Local Law Enforcement Agency
NIST – National Institute of Standards and Technology
NPP – Nuclear Power Plant
NTP – Network Time Protocol
RF – Radio Frequency
SSEP – Safety-related and important-to safety functions, Security functions, and Emergency Preparedness functions including offsite communications

2 TABLE OF CHANGES

Section 2 provides a table of changes.

TABLE 2.1 - TABLE OF CHANGES

Item #	NEI 08-09, Revision 6, Appendix	NEI 08-09, Revision 6, Section
Change # P1.01	Appendix A	Section 3.1.6
Change # P1.02	Appendix A	Section 4.3 Example 1
Change # P1.03	Appendix A	Section 4.3 Example 2
Change # P1.04	Appendix E	Section 6
Change # P1.05	Appendix A	Section 4.4.3.2
Change # P1.06	Appendix E	Section 12
Change # P1.07	Appendix D	Section 1.14
Change # P1.08	Appendix D	Section 2.5
Change # P1.09	Appendix D	Section 3.2
Change # P1.10	Appendix D	Section 3.5
Change # P1.11	Appendix D	Section 3.18
Change # P1.12	Appendix D	Section 3.20
Change # P1.13	Appendix D	Section 3.21
Change # P1.14	Appendix D	Section 1.7
Change # P1.15	Appendix D	Section 1.8
Change # P1.16	Appendix D	Section 1.9
Change # P1.17	Appendix D	Section 2.8
Change # P1.18	Appendix D	Section 1.2 and 2.2
Change # P1.19	Appendix E	Section 5
Change # P1.20	Appendix E	Section 8.5

3 CHANGE DESCRIPTION AND JUSTIFICATION

This Section provides a description and a justification for each change identified in Table 2.1. The description and justification demonstrates that the change does not decrease the effectiveness of the CSP.

Change # P1.01	Appendix A	Section 3.1.6	_

Discussion:

Appendix A, Control 3.1.6 limits the use of alternative countermeasures to a control that provides the same or greater cyber security protection which excludes controls that can provide adequate protection to meet the intent of the control. This unnecessarily limits use of controls and is more restrictive than the standard for evaluating changes to the Security Plan under 10CFR50.54(p). The proposed revision aligns the evaluation of alternative counter measures described in Appendix A Section 3.1.6 to that required by 10CFR50.54(p).

Allowance for use of NEI 13-10 should be allowed to be utilized as an alternative as allowed by CSP Section 3.1.6.

Justification:

In step 3.1.6.2, within the phrase "implementing alternative controls/countermeasures that eliminate threat/attack vectors" change "eliminate" to "mitigate the consequences of the." This change is considered to be editorial because threat/attack vectors cannot be eliminated. The threat/attack vector always exists – the controls/countermeasures are intended to address, and mitigate the threat. Therefore, this revision is a clarification to the intent, and an editorial change.

In step 3.1.6.2.b, change the phrase "provide the same or greater cyber security protection as the corresponding cyber security control" to "mitigate the threat/attack vector the control is intended to protect." This change aligns step 3.1.6.2 and 3.1.6.2.b with the intent of the action to provide protection to mitigate the threat/attack vector. The step intent is not to require an increase in protection. Therefore, this revision is a clarification to the intent, and an editorial change.

In step 3.1.6.2.c, change the phrase "that provide at least the same degree of cyber security protection as the corresponding cyber security control" to "determined in Section 3.1.6.2.b." Action 3.1.6.2.b establishes the mitigation necessary to protect the CDA and step 3.1.6.2.c should be implementing the action in 2.b and not repeat the protection criteria. Therefore, this revision is a clarification to the intent, and an editorial change.

The NRC has endorsed NEI 13-10 for use addressing cyber security controls for CDAs consistent with the methodology described in Section 3.1.6 of the Cyber Security Plan. Section 3.1.6 allows for alternative countermeasures or for not implementing security controls with justification. NEI 13-10 provides the guidance for selecting the appropriate security controls and the associated justification.

Change # P1.02	Appendix A	Section 4.3 Example 1	_

Discussion:

Appendix A, Control 4.3, Example 1, requires security communications equipment (e.g., radios and phones) to be on a level 3 or 4. NEI 08-09 Revision 6, Section 4.3 provides a defensive strategy that restricts all Security CDAs to either be air gapped or protected by a one-way deterministic boundary device (i.e., data diode). This requirement can reduce the effectiveness of the communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications. Offsite communication is with Local Law Enforcement Agency (LLEA).

Primary and backup communications between station security and the LLEA are with dedicated commercial (wired) telephone system, and LLEA radio equipment. Offsite agency communication by nature is bi-directional communication to a less secure domain that is outside of the licensee's custody and control; therefore, offsite communication systems determined to be security CDA cannot be air gapped or located behind a one-way deterministic device without reducing its effectiveness.

For onsite communication, various functions are performed by the plant telephone system such as:

- Used in radio restricted areas or otherwise not available.
- Used for communication with the control room

The plant telephone system by design is for conducting normal business communication and therefore is in a less secure domain and cannot be air-gapped or isolated behind a one-way deterministic boundary device to meet the NEI 08-09 Revision 6, Section 4.3 requirements.

Change # P1.02	Appendix A	Section 4.3 Example 1	_

Justification:

Currently, the Example 1 text requires security communications equipment (e.g., radios) to be on a level 3 or 4. NEI 08-09 Revision 6, Section 4.3 provides a defensive strategy that restricts all Security CDAs to either be air gapped or protected by a one-way deterministic boundary device (i.e., data diode). This requirement can reduce the effectiveness of the communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications. Offsite communication is with LLEA. The proposed change is being made to align the licensee CSP *Defense-in-Depth Protective Strategies*, for meeting 10CFR73.54(a)(1)(ii) *Security functions* with the Security Plan Security Communications requirements for meeting 10CFR73.55(j) *Communications requirements*.
The proposed change restores the effectiveness of the communication voice and data network capability by allowing for bi-directional communications and establishes that adequate Cyber Security Controls be provided for such digital equipment.

The proposed change does not delete or contradict regulatory requirement as described in 10CFR73.54 for Cyber Security requirement or 10CFR73.55. 10CFR73.54 and 10CFR73.55 do not stipulate that Security CDAs are air gapped or are located in levels 3 or levels 4. The proposed change still subjects the communication voice and data networks (systems) used to meet 10CFR73.55(j) to the Cyber Security Program requirements per 10CFR73.54, Cyber Security Plan.

In addition, 10CFR73.55(a)(11) states “Implementation of security plans and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions.” The defense in depth requirements for Security CDAs in NEI 08-09 Revision 6, Section 4.3 is conflicting with communication systems use by the Security organization for onsite and offsite communications as noted above.

In order to implement cyber security protective strategies for the communication voice and data networks (systems), the conflict between NEI 08-09 Revision 6 and the Security Plan requirements need to be resolved. The requirement for Security CDAs in NEI 08-09 Section 4.3 needs to be modified to allow bi-directional communications for implementation of the security communication function described above.

Change # P1.03	Appendix A	Section 4.3 Example 2	_
Discussion: Appendix A, Control 4.3, Example 2 requires security communications equipment (e.g., radios) to be on a level 3 or 4. The Discussion section for Change # P1.2 on Example 1 is applicable to Change # P1.3.			
Justification: The Justification section for Change # P1.2 on Example 1 is applicable to Change # P1.3. Deleted the phrase to require prohibiting CDAs within a common level to be on a common network. This implies all CDAs are stand alone which is impracticable.			

Change # P1.04	Appendix E	Section 6	_

Discussion:

Appendix E, Control 6 could be interpreted as requiring one-way data flow only from Level 4 to Level 3. This is not feasible in some cases where plant design requires communication between the plant data acquisition system and one or more safety-related CDAs.

Appendix E, Control 6, discusses the controls for restricting, with justification, communications from a lower security level to a higher security level. The next to last bullet includes a contradictory requirement that disallows two-way communications for a security boundary control device. This bullet defeats the purpose of installing a boundary device instead of installing a data diode. This change provides a change to Control 6 to remove this contradiction.

The proposed changes provide clarity and certainty regarding controls for data transfer between security levels. The current wording may raise questions of CSP compliance during inspections.

Justification:

The current wording (Revision 6) of Appendix E Control 6 could be interpreted as requiring one-way data flow only from Level 4 to Level 3. This is not feasible in some cases where plant design requires communication between the plant Data Acquisition System (DAS) (e.g., Plant Process Computer) and one or more safety-related CDAs. The safety-related CDAs in such a configuration "inherit" the deterministic isolation for the plant DAS. An intrusion detection/prevention scheme between the plant DAS and safety-related CDAs provides an additional measure of protection for the safety-related CDAs (protection from a plant DAS compromise also compromising the safety-related CDAs) which allows the communication to remain in-tact per plant design. The proposed language provides clarity and certainty regarding controls for data transfer between security levels. The current wording may raise questions of CSP compliance during inspections.

The current wording (Revision 6) of Appendix E Control 6, bullet 6, provides the requirement for restricting direct communications between digital assets at lower security levels and digital assets at higher security levels and providing justification that explains that communication from a less secure security level to a more secure security level verifies that a compromise of such communication will not prevent or degrade the functions performed by the CDAs in the higher security level. This provides the appropriate controls to protect the pathway from compromise of the functions performed by the CDAs. The next to last bullet is applicable to security boundary control devices and unnecessarily prevents any information flow from networks or systems at a less secure security level to a network or system at a more secure level. This additional limitation eliminates the ability to use a boundary device and restricts the interface to a data diode.

The proposed changes provide clarity and certainty regarding controls for data transfer between security levels. The current wording may raise questions of CSP compliance during inspections.

Change # P1.05	Appendix A	Section 4.4.3.2	_

Discussion:

Appendix A, Control 4.4.3.2 contains language regarding performance of vulnerability scans and the allowance for the use of vulnerability assessments or scans and the applicability to non-networked CDAs. Scanning is not always possible, and may involve possible adverse impact to SSEP functions, on CDAs in the production environment and vulnerability assessments are preferred. The proposed language provides clarity and certainty regarding these concerns.

Justification:

Security Control Appendix A 4.4.3.2 was intended for Licensees to evaluate and manage cyber risks through periodic vulnerability assessments and security scanning/testing (e.g. penetration testing, malicious user testing, vulnerability assessment testing and independent verification and validation (IV&V)). The application of this control to a nuclear power plant does not recognize Licensees are generally unable to perform any form of meaningful automated vulnerability scanning on production CDAs as Appendix A 4.4.3.2 and the Control E.12 actions specify. An initial assessment and determination of appropriate security controls is performed as part of the initial CDA assessment per CSP Sections 3.1.5 and 3.1.6. A validation and testing process is then performed the same as is done for any other plant component configuration change. Electronic scanning is intended for information networks, not industrial process indication and control networks. The requirement was added to NEI 08-09 without a sufficient consideration of the need for, the benefit of or the potential causing adverse impact at a nuclear power plant. An electronic vulnerability scan is not feasible for standalone CDAs and will not be permitted to be conducted for process indication networks because of concern about adversely impacting network operability and performance. With proper limitations, a vulnerability scans may be conducted but is not required as part of the revision to this control.

Scanning or testing (e.g. penetration testing, malicious user testing, vulnerability assessment testing and independent verification and validation (IV&V)) may cause an adverse impact to safety and important to safety, security or emergency preparedness functions. The CAP is used to manage the decision to perform an assessment or scan and the plant equipment condition to avoid adverse plant impact from the scan. The CAP evaluations should consider the threat vectors associated with the vulnerability in the decisions to conduct a scan or assessment. This change is consistent with CSP Section 3.1.6 which states, in part, “Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.” Additional guidance is added to control E.12 for conduct of assessments to enhance the guidance for conducting scans. Vulnerability notices are screened and reviewed per CSP program implementing procedures to assess new vulnerabilities that require action and are managed in CAP.

Changes are made to this section to provide clarity for when vulnerability scans or vulnerability assessments should be performed to avoid adverse impacts of SSEP functions. The revision to Section 4.4.3.2 and Appendix E Section 12 provide the alternate control(s) necessary to mitigate the lack of the vulnerability scan on an operating CDA (refer to change P1.06).

Change # P1.06	Appendix E	Section 12	_
Discussion: Appendix E, Control 12 contains controls intended for Licensees to evaluate and manage cyber risks through periodic vulnerability assessments and security testing (e.g. penetration testing, malicious user testing, vulnerability assessment testing and independent verification and validation (IV&V)). Application of the stated controls are either impracticable for production CDAs or unnecessary with application of other controls in Appendix A 4.4.2, Appendix A 4.9.1 and Appendix E.3.5.			
Justification: Refer to change P1.05 for justification of changes to A 4.4.3.2 and E.12.			

Change # P1.07	Appendix D	Section 1.14	_
Discussion: Appendix D, Control 1.14 corresponds to NIST 800-53 control AC-15 which has been withdrawn and incorporated into a different control by NIST. It is unclear what the label in D.1.14 is supposed to identify. The control does not state that the label needs to be applied automatically as the title implies. Having this control creates confusion and may raise questions of CSP compliance during inspections. This control is proposed to be deleted.			
Justification: Control D.1.14 corresponds to NIST 800-53 control AC-15 which was withdrawn by NIST. NIST 800-53 Revision 4 states that AC-15 was incorporated into MP-3. Control MP-3 is implemented in NEI 08-09 Revision 6 under E.1.3, Media Labeling/Marking. D.1.14 wording is confusing and unnecessary and is therefore deleted.			

Change # P1.08	Appendix D	Section 2.5	_
Discussion: Appendix D, Control 2.5 provides actions regarding auditing failures including shutting down a CDA. These actions may not be necessary and may cause an adverse impact to safety and important to safety, security or emergency preparedness functions. Rather, the decisions on the appropriate immediate actions to be taken are determined by the Corrective Action Program (CAP) processes. The action to shutdown a CDA is proposed to be replaced with initiation of the CAP processes to determine the appropriate immediate actions.			
Justification: Appendix D, Control 2.5 provides actions regarding auditing failures including shutting down a CDA. These actions may not be necessary and may cause an adverse impact to safety and important to safety, security or emergency preparedness functions. Changes are also made to this section to avoid adverse impacts of SSEP functions. A proposed revision to RG 5.71 Section B.2.5 was considered in this revision. This change is consistent with CSP Section 3.1.6 which states, in part, "Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions." The revision to Appendix D Section 2.5 provides the controls necessary to mitigate the audit failure. The decisions on the appropriate immediate actions to be taken are determined by the Corrective Action Program (CAP) processes.			

Change # P1.09	Appendix D	Section 3.2	_

Discussion:

Appendix D, Control 3.2 corresponds to control SC-3 in NIST 800-53. Bullets three through seven are not required by NIST 800-53 for high baseline systems such as used in Nuclear Power Plants (NPPs) and are proposed to be deleted. Licensees will primarily use the alternative control since CDAs used in the NPPs typically cannot support security function isolation. As such, the proposed change reformats the cyber security control and is considered an administrative change. The proposed language provides clarity and certainty regarding controls for security function isolation. The current wording may raise questions of CSP compliance during inspections.

Justification:

This control corresponds to control SC-3 in NIST 800-53. Bullets three through seven are not required by NIST 800-53 for high baseline systems such as used in Nuclear Power Plants (NPPs) and are proposed to be deleted. Licensees will primarily use the alternative control since CDAs used in the NPPs typically cannot support security function isolation. The controls being deleted are best practice considerations during the design process at the vendor level. These controls generally cannot be implemented by the licensee/applicant. As such, the proposed change reformats the cyber security control and is considered an administrative change. The proposed language provides clarity and certainty regarding controls for security function isolation. The current wording may raise questions of CSP compliance during inspections. In cases where the CDA does not support any security functions, this control will not be applicable

Change # P1.10	Appendix D	Section 3.5	_
Discussion: Appendix D, Control 3.5 corresponds to SC-6 in NIST 800-53. This control is only applicable in a design phase of a digital device and has been de-selected for any baseline security control.			
Justification: This control is contained in NIST 800-53 Revision 2 as control SC-6 but is not selected for any level of control and therefore is not needed to be applied. This control can only be considered for application during the initial design of a digital device. Such a control cannot be added to a digital device ready for installation or installed in the plant. Using the scoping guidance in NIST 800-53, Section 3.3, this specific control is optional and not selected for use in any baseline. Therefore this control is deleted.			

Change # P1.11	Appendix D	Section 3.18	_
Discussion: Appendix D, Control 3.18 corresponds to SC-25 in NIST 800-53, Revision 4, and was not included in Revision 2. NIST 800-53, Revision 2, was used to establish NEI 08-09, Revision 6. This control is only applicable in a design phase of a digital device and can be deleted for a baseline security control.			
Justification: This control was not contained in NIST 800-53 Revision 2 when NEI 08-09 Revision 6 was created. This control is contained in NIST 800-53 Revision 4 under control SC-25 as an enhancement. This control is not selected for any level of control and therefore is not needed to be applied. This control can only be considered for application during the initial design of a digital device that is connected to a network. A redesign of the networked CDA and associated system is necessary to implement this control. Using the scoping guidance in NIST 800-53, Section 3.2, this specific control is optional and not selected for use in any baseline. This control is not applicable to CDAs which do not have an operating system or that are stand alone. Therefore this control is deleted.			

Change # P1.12	Appendix D	Section 3.20	_

Discussion:

Appendix D, Control 3.20 corresponds to SC-29 in NIST 800-53, Revision 4, and was not included in Revision 2. NIST 800-53, Revision 2, was used to establish NEI 08-09, Revision 6. This control is only applicable in a design phase of a digital device and, per NIST 800-53, Revision 4, has been de-selected for any baseline security control. This design feature is already required by other regulations for design of a Nuclear Power Plant (e.g., General Design Criteria for single failure criterion) and adding to the CSP is redundant and beyond the intent of the Cyber Security Rule. The current wording may raise questions of CSP compliance during inspections.

Justification:

Appendix D, Control 3.20 corresponds to SC-29 in NIST 800-53, Revision 4, and was not included in Revision 2. NIST 800-53, Revision 2, was used to establish NEI 08-09, Revision 6. This control is only applicable in a design phase of a digital device and, per NIST 800-53, Revision 4, has been de-selected for any baseline security control. This design feature is already required by other regulations for design of a Nuclear Power Plant (e.g., General Design Criteria for single failure criterion) and adding to the CSP is redundant and beyond the intent of the Cyber Security Rule. The current wording may raise questions of CSP compliance during inspections.

Change # P1.13	Appendix D	Section 3.21	_
Discussion: Appendix D, Control 3.21 provides an unnecessary requirement for a licensed nuclear power plant. This change proposes deletion of a security control to protect against loss of a SSEP function from a single CDA failure. The current wording may raise questions of CSP compliance during inspections.			
Justification: Control 3.21 provides an unnecessary requirement for a licensed nuclear power plant. This change proposes deletion of a security control to protect against loss of a SSEP function from a single CDA failure. Existing NRC required design requirements for system redundancy and single failure considerations already provide protection for certain CDAs associated with safety-related and security functions as specified in a plant's Current Licensing Basis. Including this control in the CSP is redundant and beyond the intent of the Cyber Security Rule. NEI 13-10 Revision 4 recognizes that Indirect CDAs cannot have an adverse impact on or degrade SSEP functions prior to their compromise or failure being detected. NEI 13-10 Revision 4 recognizes that compromise or failure of EP CDAs would not adversely impact the ability to implement EP functions, due to the availability of alternate means of performing the EP function. The current wording may raise questions of CSP compliance during inspections. Therefore this control is deleted.			

Change # P1.14	Appendix D	Section 1.7	_
Discussion: Appendix D, Control 1.7 is silent on an alternative control for CDAs that do not support centralized logging. The format of the control in the third bullet mixes two different conditions creating ambiguous guidance. Including a specific description of an alternative control provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.			
Justification: Control D.1.7 is silent on an alternative control for CDAs that do not support centralized logging. The format of the control in the third bullet mixes two different conditions creating ambiguous guidance. An alternative control is provided where the CDA does not support centralized logging and relies on physical protection and oversight by an independent individual. Including a specific description of an alternative control provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.			

Change # P1.15	Appendix D	Section 1.8	_
Discussion: Appendix D, Control 1.8 does not provide guidance if application of the System Use Notification could have an adverse impact on performance, safety, or reliability. Including a specific description of an alternative control provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.			
Justification: Control D.1.8 does not provide guidance if application of the System Use Notification could have an adverse impact on performance, safety, or reliability. Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions. Per CSP Section 3.1.6, when a cyber security control is determined to have an adverse effect, alternate controls are used. The control is revised to provide specific description of an alternative control where System Use notifications are not possible on the CDA. Including a specific description of an alternative control provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.			

Change # P1.16	Appendix D	Section 1.9	_

Discussion:

Appendix D, Control 1.9 does not distinguish use of this control when notification message has an adverse impact on performance, safety, or reliability and cannot be implemented without impacting the current design configuration of the CDA. Including a specific control description that also provides an alternative control provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.

Justification:

Control D.1.9 does not provide guidance if application of the Previous Logon Notification could have an adverse impact on performance, safety, or reliability. Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions. Per CSP Section 3.1.6, when a cyber security control is determined to have an adverse effect, alternate controls are used. The control is revised to provide specific description of an alternative control where Previous Logon Notifications are not possible on the CDA. Including a specific description for an alternative control provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.

Windows operating systems prior to Windows Vista do not support previous logon notifications. For Windows Vista and later windows Operating Systems, modifications need to be performed to the local group policies to enable this feature. For existing systems that use Windows Vista or later OSs, this would require a design change. CDAs that use active directories have to be using Windows 2008 server in order to support previous logon notification. These considerations should be taken into when implementing this control.

Change # P1.17	Appendix D	Section 2.8	_
Discussion: Appendix D Control 2.8 should allow use of a GPS-linked time source that is trusted and secure. The current wording may raise questions of CSP compliance during inspections.			
Justification: The addition of the use of a GPS-based time server is secure for a couple of reasons. First, this option uses an RF carrier with digitally encoded GPS data to determine time. The NTP server does see the location of the antenna, but this would only be used to determine time zone. The main two possible exploits are going to be spoofing and denial of service. A Denial of Service could be accomplished easily by simply broadcasting noise in the 1.5 GHz range (up to a half mile away) overpowering the GPS signal. This becomes a moot point however in the fact that if time signal is lost, or the NTP server throws it out due to satellite quorum differences, the NTP server is going to run using the internal holdover clock (Rubidium clock source with less than 1ms drift over a 1 year time frame). While spoofing the GPS is possible, it is highly unlikely due to the needed proximity to the antenna and complexity in doing it. Additionally, the coax input into the NTP server is an input only and does not have the ability to transmit. Therefore, the use of digitally encoded GPS data to determine time is sufficiently secure for use. The proposed language provides clarity and certainty regarding controls for data transfer between security levels. The current wording may raise questions of CSP compliance during inspections.			

Change # P1.18	Appendix D	Section 1.2 and 2.2	_
Discussion: Appendix D, Control 1.2 has two primary purposes: 1. Manage accounts on a CDA so that only authorized, necessary or appropriate user accounts or account privileges exist on a CDAs as to reduce the possibility of such accounts being misused for malicious purposes; and, 2. Periodically review accounts on CDAs to ensure that only authorized and necessary accounts exist. This control does not distinguish between CDAs that use and do not use central account management capabilities. Alternative controls are included for both specific cases thus providing clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections. The review frequency is adjusted based on site operating experience and work management processes.			

Change # P1.18	Appendix D	Section 1.2 and 2.2	_

Justification:

Appendix D, Control 1.2 has two primary purposes: 1. Manage accounts on a CDA so that only authorized, necessary or appropriate user accounts or account privileges exist on a CDAs as to reduce the possibility of such accounts being misused for malicious purposes; and, 2. Periodically review accounts on CDAs to ensure that only authorized and necessary accounts exist. This control does not distinguish between CDAs that use and do not use central account management capabilities. Alternative controls are included for both specific cases thus providing clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections. Per CSP Section 3.1.6.2.d, the frequency is adjusted based on site operating experience and work management processes.

Authorizing, establishing and activating accounts on CDAs is controlled through station procedures/process Sites have processes in place to ensure that unnecessary accounts such as temporary, guest and emergency accounts are not created on an operational CDA.

Modifying, disabling, and removing accounts can only be accomplished following station procedure/process. Additionally automatically disabling and terminating accounts may have an adverse effect on SSEP functions.

Majority of the CDAs in question are not logically accessed every 31 days and therefore accounts may remain inactive for up to 2 years. Disabling accounts after 31 days of inactive may lead to unnecessarily denying access to a CDA. Accounts that are granted for a short-term (e.g., < 30 days) are reviewed every 31 days for removal.

Majority of the CDAs in the plant do not support centralized account management and do not support the number of individual accounts necessary to allow individuals in the Maintenance Departments to work on a CDA. Accounts on these CDAs are setup as group accounts where access to the CDA and account passwords is controlled through the work management process.

The revised control requires that where a centralized account management system does not exist, accounts will be reviewed any time the CDA is accessed where a potential exists to modify the configuration of an account.

Control for creating and protecting audit records is relocated from D.1.2 to D.2.2.

Change # P1.19	Appendix E	Section 5	_

Discussion:

Appendix E, Control 5.1 states the scope is for CDAs outside the protected area. The other controls in Section E5 do not have this similar scope limitation. Suggest adding the scope limit in E5.1 to the full family of security controls in Section E5.

This security control is written to provide operational environmental protection for CDAs. The only specific security control that stipulates requirements for environmental controls is E.5.3 and calls for preventing degradation of the operational environment which could impact the correct performance of CDAs (e.g., by temperature, humidity, dust, vibration, and electromagnetic interference or radio frequency interference). Consideration of environmental impacts that could adversely impact SSEP functions is part of the CDA scoping process and is not needed as a specific control. Suggest removing the operational environmental protection aspects from Section E.5.

Justification:

For CDAs inside the Protected Area, requirements in the Physical Security Plan to comply with 10CFR73.55 provide sufficient cyber security controls to provide adequate protection for the E.5 security controls. An introduction to Section 5 is provided to reinforce that the entire family of security controls under Appendix E Section 5 are applicable to CDAs located outside the Protected Area.

This security control is written to provide operational environmental protection for CDAs. The only specific security control that stipulates requirements for environmental controls is E.5.3 and calls for preventing degradation of the operational environment which could impact the correct performance of CDAs (e.g., by temperature, humidity, dust, vibration, and electromagnetic interference or radio frequency interference). NEI 10-04 Section 2.4 provides guidance for classifying support equipment as CDAs if the support equipment is required to provide a stable environment conducive to the operational requirements of systems associated with SSEP functions. Per NEI 10-04 and CSP Appendix A Section 3.1.3, such support equipment would be classified as a CDA and then security controls would be determined and applied per CSP Appendix A Section 3.1.6. This ensures the necessary security controls are applied to ensure the adverse environment conditions are prevented from having an adverse impact on SSEP functions. Security control 5.1 and 5.3 are revised to remove environmental protection language.

Change # P1.20	Appendix E	Section 8.5	_
Discussion: Appendix E, Control 8.5 in part requires verifying media reliability and information integrity on a monthly basis which is inappropriate to be generically applied to all types of media. This change proposes an interval that is based on the long-term integrity of the particular storage media. Including a more appropriate control description provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections.			
Justification: Control E.8.5 in part requires verifying media reliability and information integrity on a monthly basis which is inappropriate to be generically applied to all types of media. Imposing a single interval for all media types is inappropriate since long-term data integrity for some media types is much better that for other types of media. This change proposes an interval that is identified in licensee's procedures and justified according to the licensee's assessment to verify media reliability and information integrity. The frequency of the verification is to be controlled in licensee's procedures based on industry experience or vendor recommendations for the specific media. Other requirements in this control protect the CDA from intentional tampering. Including a more appropriate control description provides clarity and certainty regarding assessment of this control. The current wording may raise questions of CSP compliance during inspections. Per CSP Section 3.1.6.2.d, the frequency is adjusted based on new technology and industry operating experience with more reliable and longer lasting data storage media.			

END

4 CHANGES WITH REVISION MARKERS

This Section provides a 'red-line/strike-out' to the applicable sections in NEI 08-09, Revision 6. The changes show additions with **red bolded text** and deletions with ~~red strikethrough text~~.

Change # P1.01	Appendix A	Section 3.1.6	_

Proposed CSP Text:

For CDAs, the information in Sections 3.1.3 - 3.1.5 is utilized to analyze and document one or more of the following ~~:~~ **actions. NEI 13-10 may be used to satisfy the actions in 3.1.6.**
1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.
2. Implementing alternative controls/countermeasures that ~~eliminate~~ **mitigate the consequences of the** threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1)
above by:
a. Documenting the basis for employing alternative countermeasures;
b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures ~~provide the same or greater cyber security protection as the corresponding cyber security control~~ **mitigate the threat/attack vector the control is intended to protect**; and
c. Implementing alternative countermeasures **determined in Section 3.1.6.2.b** ~~that provide at least the same degree of cyber security protection as the corresponding cyber security control~~;
d. Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:
i. NRC Regulations, Orders
ii. Operating License Requirements (e.g., Technical Specifications)
iii. Site operating history
iv. Industry operating experience
v. Experience with security control
vi. Guidance in generally accepted standards (e.g., NIST, IEEE, ISO)
vii. Audits and Assessments
viii. Benchmarking
ix. Availability of new technologies.
3. Not implementing one or more of the cyber security controls by:
a. Performing an analysis of the specific cyber security controls for the CDA that will not be implemented
b. Documenting justification demonstrating the attack vector does not exist (i.e., not applicable) thereby demonstrating that those specific cyber security controls are not necessary.

Change # P1.02	Appendix A	Section 4.3 Example 1	_

Proposed CSP Text

Example 1:

The site defensive model implements all of the following:

- The defensive model consists of 4 layers, with layer 4 having the greatest level of protection.
- Safety CDAs are in Level 4.
- ~~Security CDAs are in Levels 4 and 3~~**Security CDAs are air gapped or are located behind a unidirectional deterministic boundary device with the exception of communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications that require bi-directional communication to meet regulatory and plan requirements.**
- The boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above Level 3.Information flows between Level 3 and 4 are restricted through the use of a firewall and network- based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6, Appendix D, Section 1.4 and the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 6, Appendix E, Section 6.

Change # P1.03	Appendix A	Section 4.3 Example 2	_

Proposed CSP Text

Example 2:

The site defensive model implements all of the following:

- The defensive model consists of 4 layers, with layer 4 having the greatest level of protection.
- Safety CDAs are in Level 4.
- ~~Security CDAs are in Levels 4 and 3~~.
- ~~CDAs within a particular security level may not share a common network.~~
- Safety CDAs are isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air-gaps).
- ~~Security CDAs are isolated from all other CDAs by a defensive boundary that implement the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 6, Appendix E, Section 6~~. **Security CDAs are air gapped or are located behind a unidirectional deterministic boundary device with the exception of communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications that require bi-directional communication to meet regulatory and plan requirements.**
- Information flows between Security CDAs in one level and Security CDAs in another level are restricted through the use of a firewall and network-based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6, Appendix D, Section 1.4.

]

Change # P1.04	Appendix E	Section 6	_

Proposed CSP Text

6 DEFENSE-IN-DEPTH

This security control implements and documents a defensive strategy that:

- Allocates the appropriate degree (i.e., level 4, 3, etc.) of cyber security protection to CDAs that carry out safety, important-to-safety, security, and emergency preparedness functions, and protect those CDAs from lower defensive levels.
- Controls/restricts remote access to CDAs located in the highest defensive level.
- Allocates at least the second highest degree of cyber security protection (i.e., level 3) to CDAs providing data acquisition functions and protect those CDAs from lower defensive levels.
- Allows only one-way direct data flow from **the more secure**~~higher security levels~~ to **less secure**~~lower~~ security levels **in accordance with Section 4.3 of the licensee's CSP**.
- Ensures that data flow from one level to other levels occurs through a device that enforces the security policy between levels and detect, prevent, delay, mitigate, and recover from a cyber attack coming from the lower security level.
- Ensures that direct communications between digital assets at lower security levels and digital assets at higher security levels are eliminated or restricted with justification that explains that communication from a lower security level to a higher security level verifies that a compromise of such communication will not prevent or degrade the functions performed by the CDAs in the higher security level.
- Moves data, software, firmware and devices from lower levels of security to higher levels of security using a documented validation process or procedure. The validation process or procedure is trustworthy at or above the trusted level of the device the data, code, information or device is installed on or connected with to ensure that the data, software, firmware or devices are free from known malicious code, Trojans viruses, worms and other passive attacks.

In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:

…[no changes to other bullets]

- Uses physically and logically secured and hardened computing devices and flow control to prevent unauthorized access, or manipulation of data streams;
- Allows no information of any kind, including handshaking protocols, to be transferred directly **(i.e., without traversing the boundary control device)** from networks or systems existing at the ~~lower security~~ **less secure** level to networks or systems existing at the ~~higher security~~ **more secure** level;
- Employs measures to prevent viruses or other malicious or unwanted programs from propagating information between security levels.

Change # P1.05	Appendix A	Section 4.4.3.2	_

Proposed CSP Text

4.4.3.2 Vulnerability Assessments and Scans

Vulnerability assessments or e~~E~~lectronic vulnerability scanning of CDAs **are** performed **as described in Appendix E, 12, "Evaluate and Manage Cyber Risk,"** when ~~security controls are first applied, and as required by specific guidance in the cyber security controls in Appendixces D and E of NEI 08-09, Revision 6. When~~ new vulnerabilities that could affect the cyber security posture of CDAs are identified~~, vulnerability scanningwill be performed~~.

When new vulnerabilities are discovered, the issue is documented in the Corrective Action Program (CAP). CAP evaluations should consider the threat vectors associated with the vulnerability. Vulnerabilities that pose a risk to SSEP functions are mitigated when the CAP evaluation concludes remediation is required to maintain adequate defense-in-depth. ~~Vulnerability scan reports are analyzed and vulnerabilities that could result in a risk to SSEP functions at the site are remediated.~~ Information obtained from the vulnerability **assessment or** scanning process is shared with appropriate personnel to ensure that similar vulnerabilities that may impact interconnected or similar CDA(s) are understood, evaluated and mitigated.

Prior to performing vulnerability scans, ~~When there is a~~ risk of operational disruption **must be considered**. **The assessment and scanning process must not adversely impact SSEP functions. If this could occur, CDAs are removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. Scans should be** ~~electronic vulnerability scans are~~ conducted during **scheduled outage** periods ~~of scheduled outage~~. **Development or** ~~T~~**t**est beds **or**~~and~~ vendor maintained environments may be used **to** ~~for or in substitution for~~ **perform**~~ing~~ vulnerability scans.

~~Assessment and scanning process must not adversely impact SSEP functions. If this could occur, CDAs are removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. If vulnerability assessments or scanning cannot be performed on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls (e.g., providing a replicated system or CDA to conduct scanning) are employed.~~

~~A vulnerability assessment may be used as a substitute for vulnerability scanning where there is risk of an adverse impact to SSEP functions,~~ **or**~~and when off-line, replicated, or vendor test beds are not available. When new vulnerabilities are discovered, the vulnerability assessment considers the same threat vectors as the identified vulnerabilities. When vulnerability assessments are used to verify security controls, the assessment targets the threat vectors the security controls address. In both cases, the vulnerability assessment verifies that the vulnerability or threat vector is addressed to provide high assurance of adequate protection that SSEP functions are protected from cyber attacks up to and including the Design Basis Threat.~~

Change # P1.06	Appendix E	Section 12	_

Proposed CSP Text

This security control consists of establishing, implementing and documenting requirements to evaluate and address the following:

- **Screen for applicable** ~~Scan or assess for~~ **CDA** vulnerabilit~~yies~~ ~~in the CDAs~~ **notices** no less frequently than every 92 days, and at random intervals, and as necessary when new vulnerabilities affecting the CDAs are identified and reported;

For CDA Vulnerability Assessments:

- **Ensure configuration information used to identify applicable cyber threats and vulnerabilities is accurate and updated when new CDAs are installed and placed into production.**
- **Ensure applicable threat and vulnerability information for CDAs is entered into the licensee Corrective Action Program (CAP) and evaluated in accordance with the fleet/site process.**
- **Ensure identified corrective actions required to mitigate threat vectors associated with applicable threat and vulnerability notifications and maintain adequate defense-in-depth are documented and tracked in CAP.**

For CDA Vulnerability Scans, licensees should perform the following activities to the extent possible:

- Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting and making transparent, checklists and test procedures; and
  - Measuring vulnerability impact;
- Analyze vulnerability scan reports and remediates legitimate vulnerabilities and organizational assessment of risk; and
- Share information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.
- Employ vulnerability scanning tools that include the capability to update the list of cyber vulnerabilities scanned and updates the list of information system vulnerabilities scanned at a maximum frequency as defined in the risk determination or as necessary when new vulnerabilities are identified and reported.
- Attempt to discern what information about the information system is discoverable by adversaries.
- Perform security testing to determine the level of difficulty in circumventing the security controls of the CDAs. Testing methods may include: penetration testing, malicious user testing, and independent verification and validation (IV&V).
- Include privileged access authorization to CDAs for selected vulnerability scanning activities to facilitate more thorough scanning.
- Employ automated mechanisms to detect the presence of unauthorized software on CDAs and notifies authorized personnel.
- Review historic audit logs to determine if a vulnerability identified in the CDA has been previously exploited.

Change # P1.07	Appendix D	Section 1.14	_
Proposed CSP Text **D1.14 AUTOMATED LABELING** **DELETED**~~This Technical cyber security control ensures hard and soft copy information in storage, in process, and in transmission is labeled.~~			

Change # P1.08	Appendix D	Section 2.5	_

Proposed CSP Text

2.5 Response To Audit Processing Failures

This Technical cyber security **control manages responses to audit processing failures by performing the following**:

- ~~Ensures CDAs provide a warning when allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity, which is based on the function of how quickly storage capacity is consumed, and documents the organization's resources and response times.~~
- ~~Ensures justification and details of alternate compensating security controls are documented where a CDA cannot respond to audit processing failures.~~
- ~~Responses to audit failures include the use of an external system to provide these capabilities.~~
- ~~If audit processing capabilities fail for a CDA or security boundary device, the following occurs:~~
  - ~~Alerts are sent to designated officials in the event of an audit processing failure.~~
  - ~~Auditing failures are treated as a failure of the CDA or security boundary device~~
  - ~~Ensures CDAs with auditing failures take the following additional actions:~~
    1. ~~Shut down the CDA,~~
    2. ~~Failover to a redundant CDA, where necessary to prevent adverse impact to safety, security or emergency preparedness functions,~~
    3. ~~Overwrite, when necessary, the oldest audit record(s), and~~
    4. ~~Stop generating audit records.~~
- **For CDAs that are part of centralized logging, if audit processing capabilities fail for a CDA or security boundary device, alerts are sent to designated officials.**
- **If the design configuration of the CDA's supports, provide a warning when allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity. The storage volume limit is based on the function of how quickly storage capacity is consumed and the organization's resources and response times.**
- **Actions are taken to preserve the audit logs for record retention requirements and after-the-fact investigations.**
- **Auditing failures will be assessed and determination of the device functionality should follow the CAP process.**
- **Justification and details for alternate compensating security controls are documented for those instances in which a CDA cannot respond to audit processing failures.**

Change # P1.09	Appendix D	Section 3.2	_

Proposed CSP Text

3.2 Application Partitioning/Security Function Isolation

This Technical cyber security control:

- Configures CDAs to separate applications into user functionality (including user interface services) and CDAs management functionality.
- Configures CDAs to isolate security functions from non-security functions. This is accomplished through partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform these security functions.
- ~~Configures CDAs to employ underlying hardware separation mechanisms to facilitate security function isolation.~~
- ~~Configures CDAs to isolate critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and other security functions.~~
- ~~Configures CDAs to minimize the number of non-security functions included within the isolation boundary containing security functions.~~
- ~~Configures CDAs security functions as independent modules that avoid unnecessary interactions between modules.~~
- ~~Configures CDAs security functions as a layered structure minimizing interactions between levels of the design and avoid any dependence by lower levels on the functionality or correctness of higher levels, or~~
- ~~Implements alternative controls and documents the justification for alternative controls/countermeasures~~ **W**~~w~~here a CDA cannot support security function isolation **implements alternative physical controls, such as**~~and implements the following~~:
    - Physically restricts access to the CDA,
    - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
    - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
    - Ensures that individuals who have access to the CDA are qualified, and
    - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

Change # P1.10	Appendix D	Section 3.5	_
Proposed CSP Text **3.5 Resource Priority** **DELETED**~~This Technical cyber security control configures CDAs to limit the use of resources by priority thus preventing lower-priority processes from delaying or interfering with the CDAs servicing of any higher-priority process.~~			

Change # P1.11	Appendix D	Section 3.18	_
Proposed CSP Text **3.18 Thin Nodes** **DELETED**~~This Technical cyber security control configures CDAs and consoles to employ processing components that have minimal functionality and data storage.~~			

Change # P1.12	Appendix D	Section 3.20	_
Proposed CSP Text **3.20 Heterogeneity** **DELETED** ~~This Technical cyber security control employs diverse information technologies in the implementation of CDAs.~~			

Change # P1.13	Appendix D	Section 3.21	_

Proposed CSP Text

3.21 Fail In Known (Safe) State

DELETED ~~This cyber security control ensures the following:~~

- ~~CDAs fail in a state that ensures that SSEP functions are not adversely impacted by the CDA's failure, and~~
- ~~A loss of availability, integrity, or confidentiality, in the event of a failure of the CDA or a component of the CDA is prevented.~~

Change # P1.14	Appendix D	Section 1.7	_

Proposed CSP Text

1.7 Unsuccessful Login Attempts

This Technical cyber security control:

- Implements security controls to limit the number of invalid access attempts by a user and documented this requirement in the access control policy. The number of failed user login attempts per specified time period may vary by CDA. For example, greater than three (3) invalid attempts within a one (1) hour time period automatically locks out the account. The system enforces the lock out mode automatically.
- Ensures that accounts can only be unlocked by authorized individuals who are not the locked out user when the maximum number of unsuccessful login attempts has been exceeded, and documents this requirement in the access control policy. Alternatively, use of other verification techniques or mechanisms which incorporate identity challenges may be used.
- Documents the justification and details for alternative controls/countermeasures where a CDA cannot support account/node locking or delayed login attempts **where CDAs do not support centralized logging:**
  - **Alternative controls/countermeasures are employed including: 24x7 monitoring, located in a Vital Area, located within a Locked Cabinet, or other physical control.**
- **Where** a CDA cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, alternative controls/countermeasures are employed to include:
  - Real time logging and recording of unsuccessful login attempts.
  - Real time alerting of designated personnel with the security expertise for the CDA through alarms when the number of defined consecutive invalid access attempts is exceeded.

Change # P1.15	Appendix D	Section 1.8	_

Proposed CSP Text

1.8 **System Use Notification**

This Technical cyber security control:

- **Where the design of the CDA supports the use of System Use Notification message and implementation does not have an adverse impact on the SSEP function;**
  - Displays a "System Use Notification" message before granting system access informing potential users:
    - That the user is accessing a restricted system.
    - That system usage may be monitored, recorded, and subject to audit.
    - That unauthorized use of CDAs is prohibited and subject to criminal and civil penalties, and
    - That the use of CDAs indicates consent to monitoring and recording.
  - Ensures that CDA "System Use Notification" message provides privacy and security notices.
  - Approves CDA "System Use Notification" message before its use.
  - Ensures that CDA "System Use Notification" message remains on the screen until the user takes explicit actions to log on to the CDA.
- Installs physical notices ~~where a CDA cannot support System Use Notifications.~~ **at a central location to inform plant personnel of the potential consequences of unauthorized access to CDAs where System Use Notifications are not provided on the CDA.**

Change # P1.16	Appendix D	Section 1.9	_

Proposed CSP Text

1.9 Previous Logon Notification

This Technical cyber security control:

- **If the current design configuration of the CDA's operating system supports previous logon notification, then** ~~C~~configures CDAs, upon successful logon, to display the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.
- Administratively requires end users to report any suspicious activity to the Cyber Security Program Manager.

Change # P1.17	Appendix D	Section 2.8	_

Proposed CSP Text

2.8 TIME STAMPS

This Technical cyber security control ensures CDAs use a time source protected at an equal or greater level than the CDAs or internal system clocks to generate time stamps for audit records, and the time on CDAs are synchronized.

The time of CDAs are synchronized from a dedicated source protected at an equal or greater level than the CDA existing on the security network, attached directly to the CDA, **via a GPS-based time server** or via SNTP and a trusted key management process.

Only methods of time synchronization that do not introduce a vulnerability to cyber attack and/or common-mode failure are utilized, or alternative controls are implemented to manage potential cyber security risks when time synchronization cannot be used for a CDA.

Change # P1.18	Appendix D	Section 1.2 and 2.2	_

Proposed CSP Text

1.2 Account Management

This Technical cyber security control:

- Manages and documents CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts.
- Reviews CDA accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on **temporary granted** CDA accounts at least every 31 days.
- ~~Requiring access rights to be job function based.~~
- ~~Conducting reviews when as individuals job function changes to ensure that rights remain limited to the individuals job function.~~
- ~~Employs computerized mechanisms that support CDA account management functions. The CDA will automatically:~~
    - ~~Terminate temporary, guest, and emergency accounts within a maximum time period of inactivity at least every 31 days.~~
    - ~~Disable inactive accounts within 31 days.~~
    - ~~Create and protect audit records for account creation, deletion and modification,~~
    - ~~Document and notify system administrators of account creation, deletion and modification activities. This is to make system administrators aware of any account modifications and can investigate potential cyber attacks.~~
- **Licensee policies/procedures shall not allow temporary, guest, and emergency accounts unless their use is documented.**
- **Accounts on CDAs (Group or individual) shall only be authorized/terminated through station policies/procedures.**
- **Requiring access rights to be job function based.**
- **Any unauthorized accounts identified through an audit on a CDA will be documented in CAP for resolution.**

For CDAs that do not utilize Centralized Account Management

- **CDAs will use common role based group accounts to the extent possible. (Admin, User, Maintenance)**
- **Accounts will be used to enforce least privilege**
- **As a minimum, Accounts will be reviewed during maintenance/design activities where root/privileged level access is required.**
- **If individuals are granted unique access rights, then conduct reviews as individual's job function changes to ensure that rights remain limited to the individual's job function.**

For CDAs that use utilize Centralized Account Management

- **Accounts will be reviewed every 31 days.**
- **Conduct reviews when as individual's job function changes to ensure that rights remain limited to the individual's job function.**

2.2 Auditable Events [insert new bullet from D1.2 as last bullet in D 2.2]

- **Create and protect audit records for account creation, deletion and modification,**

Change # P1.19	Appendix E	Section 5	_

Proposed CSP Text

5 PHYSICAL ~~AND OPERATIONAL ENVIRONMENT~~ PROTECTION

This family of security controls implements and documents physical protections for CDAs located outside the protected area. Physical protections for CDAs located inside the protected area are provided by the Physical Security Plan to comply with 10CFR73.55.

5.1 PHYSICAL ~~AND OPERATIONAL ENVIRONMENT~~ PROTECTION POLICIES AND PROCEDURES

This security control ~~For those CDAs located outside of the protected area,~~ develop**s**, implement**s**, review**s** in accordance with 10 CFR 73.55(m), and update**s**:

- A formal, documented physical ~~and operational environment~~ protection policy that addresses:
  - The purpose of the physical security program as it relates to protecting the CDAs;
  - The scope of the physical security program as it applies to the organization's staff and third-party contractors;
  - The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with security policies and other regulatory commitments.
- Formal, documented procedures to facilitate the implementation of the physical ~~and operational environment~~ protection policy and associated physical ~~and operational environmental~~ protection security controls.

5.2 THIRD PARTY/ESCORTED ACCESS

This security control consists of:

- Screening, enforcing and documenting security controls for third-party personnel and monitoring service provider behavior and compliance. Third-party providers include service contractors and other organizations providing control system operation and maintenance, development, IT services, outsourced applications, and network and security management.
- Including personnel security controls in acquisition-related contract and agreement documents.

5.3 PHYSICAL ~~& ENVIRONMENTAL~~ PROTECTION

This security control consists of securing and documenting physical access to CDAs. Physical security controls (e.g., physically isolate environment, locked doors, etc.) are employed to limit access to CDAs ~~and to prevent degradation of the operational environment which could impact the correct performance of CDAs (e.g., by temperature, humidity, dust, vibration, and electromagnetic interference or radio frequency interference)~~.

[Remainder of Section E.5 is unchanged.]

Change # P1.20	Appendix E	Section 8.5	_

Proposed CSP Text

8.5 CDA BACKUPS

This security control consists of:

- Conducting backups of user-level and system-level information.
- Backing up CDAs at an interval identified for the CDA or based on trigger events.
- Protecting backup information at the storage location.
- Testing and documenting backup information at an interval identified **in the licensee's procedures and justification is provided for the interval according to the licensee's assessment** ~~by the no less than every 31 days~~ to verify media reliability and information integrity.
- Using backup information in the restoration of CDAs functions as part of contingency plan testing.
- Protecting system backup information from unauthorized modification
- Storing backup copies of the operating system and other critical CDA software in a separate facility or in a fire-rated container that is not co-located with the operational software.
- Establishing and documenting the timeframe in which data or the CDA must be restored and the frequency at which critical data and configurations are changing.

END

5 CHANGES WITH FINAL TEXT

This Section provides the final text of the revised NEI 08-09, Revision 6, incorporating the changes identified in Section 4. The changes show only additions as **red bolded** text.

Change # P1.01	Appendix A	Section 3.1.6	_

Proposed CSP Text:

For CDAs, the information in Sections 3.1.3 - 3.1.5 is utilized to analyze and document one or more of the following **actions. NEI 13-10 may be used to satisfy the actions in 3.1.6.**
1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.
2. Implementing alternative controls/countermeasures that **mitigate the consequences of the** threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1)
above by:
a. Documenting the basis for employing alternative countermeasures;
b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures **mitigate the threat/attack vector the control is intended to protect**; and
c. Implementing alternative countermeasures **determined in Section 3.1.6.2.b**;
d. Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:
i. NRC Regulations, Orders
ii. Operating License Requirements (e.g., Technical Specifications)
iii. Site operating history
iv. Industry operating experience
v. Experience with security control
vi. Guidance in generally accepted standards (e.g., NIST, IEEE, ISO)
vii. Audits and Assessments
viii. Benchmarking
ix. Availability of new technologies.
3. Not implementing one or more of the cyber security controls by:
a. Performing an analysis of the specific cyber security controls for the CDA that will not be implemented
b. Documenting justification demonstrating the attack vector does not exist (i.e., not applicable) thereby demonstrating that those specific cyber security controls are not necessary.

Change # P1.02	Appendix A	Section 4.3 Example 1	_

Proposed CSP Text

Example 1:

The site defensive model implements all of the following:

- The defensive model consists of 4 layers, with layer 4 having the greatest level of protection.
- Safety CDAs are in Level 4.
- **Security CDAs are air gapped or are located behind a unidirectional deterministic boundary device with the exception of communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications that require bi-directional communication to meet regulatory and plan requirements.**
- The boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above Level 3.Information flows between Level 3 and 4 are restricted through the use of a firewall and network- based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6, Appendix D, Section 1.4 and the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 6, Appendix E, Section 6.

Change # P1.03	Appendix A	Section 4.3 Example 2	_

Proposed CSP Text

Example 2:

The site defensive model implements all of the following:

- The defensive model consists of 4 layers, with layer 4 having the greatest level of protection.
- Safety CDAs are in Level 4.
- Safety CDAs are isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air-gaps).
- **Security CDAs are air gapped or are located behind a unidirectional deterministic boundary device with the exception of communication voice and data networks (systems) used by the Security organization to meet 10CFR73.55(j) (*Communication requirements*) and Security Plan requirements for onsite and offsite communications that require bi-directional communication to meet regulatory and plan requirements.**
- Information flows between Security CDAs in one level and Security CDAs in another level are restricted through the use of a firewall and network-based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6, Appendix D, Section 1.4.

]

Change # P1.04	Appendix E	Section 6	_

Proposed CSP Text

6 DEFENSE-IN-DEPTH

This security control implements and documents a defensive strategy that:

- Allocates the appropriate degree (i.e., level 4, 3, etc.) of cyber security protection to CDAs that carry out safety, important-to-safety, security, and emergency preparedness functions, and protect those CDAs from lower defensive levels.
- Controls/restricts remote access to CDAs located in the highest defensive level.
- Allocates at least the second highest degree of cyber security protection (i.e., level 3) to CDAs providing data acquisition functions and protect those CDAs from lower defensive levels.
- Allows only one-way direct data flow from **the more secure** to **less secure** security levels **in accordance with Section 4.3 of the licensee's CSP**.
- Ensures that data flow from one level to other levels occurs through a device that enforces the security policy between levels and detect, prevent, delay, mitigate, and recover from a cyber attack coming from the lower security level.
- Ensures that direct communications between digital assets at lower security levels and digital assets at higher security levels are eliminated or restricted with justification that explains that communication from a lower security level to a higher security level verifies that a compromise of such communication will not prevent or degrade the functions performed by the CDAs in the higher security level.
- Moves data, software, firmware and devices from lower levels of security to higher levels of security using a documented validation process or procedure. The validation process or procedure is trustworthy at or above the trusted level of the device the data, code, information or device is installed on or connected with to ensure that the data, software, firmware or devices are free from known malicious code, Trojans viruses, worms and other passive attacks.

In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:

…[no changes to other bullets]

- Uses physically and logically secured and hardened computing devices and flow control to prevent unauthorized access, or manipulation of data streams;
- Allows no information of any kind, including handshaking protocols, to be transferred directly **(i.e., without traversing the boundary control device)** from networks or systems existing at the **less secure** level to networks or systems existing at the **more secure** level;
- Employs measures to prevent viruses or other malicious or unwanted programs from propagating information between security levels.

Change # P1.05	Appendix A	Section 4.4.3.2	_

Proposed CSP Text

4.4.3.2 Vulnerability Assessments and Scans

Vulnerability assessments or electronic vulnerability scanning of CDAs **are** performed **as described in Appendix E, 12, "Evaluate and Manage Cyber Risk,"** when new vulnerabilities that could affect the cyber security posture of CDAs are identified.

When new vulnerabilities are discovered, the issue is documented in the Corrective Action Program (CAP). CAP evaluations should consider the threat vectors associated with the vulnerability. Vulnerabilities that pose a risk to SSEP functions are mitigated when the CAP evaluation concludes remediation is required to maintain adequate defense-in-depth. Information obtained from the vulnerability **assessment or** scanning process is shared with appropriate personnel to ensure that similar vulnerabilities that may impact interconnected or similar CDA(s) are understood, evaluated and mitigated.

Prior to performing vulnerability scans, risk of operational disruption **must be considered**. **The assessment and scanning process must not adversely impact SSEP functions. If this could occur, CDAs are removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. Scans should be** conducted during **scheduled outage** periods. **Development or t**est beds **or** vendor maintained environments may be used **to perform** vulnerability scans.

Change # P1.06	Appendix E	Section 12	_

Proposed CSP Text

This security control consists of establishing, implementing and documenting requirements to evaluate and address the following:

- **Screen for applicable CDA** vulnerabilit**y notices** no less frequently than every 92 days, and at random intervals, and as necessary when new vulnerabilities affecting the CDAs are identified and reported;

For CDA Vulnerability Assessments:

- **Ensure configuration information used to identify applicable cyber threats and vulnerabilities is accurate and updated when new CDAs are installed and placed into production.**
- **Ensure applicable threat and vulnerability information for CDAs is entered into the licensee Corrective Action Program (CAP) and evaluated in accordance with the fleet/site process.**
- **Ensure identified corrective actions required to mitigate threat vectors associated with applicable threat and vulnerability notifications and maintain adequate defense-in-depth are documented and tracked in CAP.**

For CDA Vulnerability Scans, licensees should perform the following activities to the extent possible:

- Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting and making transparent, checklists and test procedures; and
  - Measuring vulnerability impact;
- Analyze vulnerability scan reports and remediates legitimate vulnerabilities and organizational assessment of risk; and
- Share information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.
- Employ vulnerability scanning tools that include the capability to update the list of cyber vulnerabilities scanned and updates the list of information system vulnerabilities scanned at a maximum frequency as defined in the risk determination or as necessary when new vulnerabilities are identified and reported.
- Attempt to discern what information about the information system is discoverable by adversaries.
- Perform security testing to determine the level of difficulty in circumventing the security controls of the CDAs. Testing methods may include: penetration testing, malicious user testing, and independent verification and validation (IV&V).
- Include privileged access authorization to CDAs for selected vulnerability scanning activities to facilitate more thorough scanning.
- Employ automated mechanisms to detect the presence of unauthorized software on CDAs and notifies authorized personnel.
- Review historic audit logs to determine if a vulnerability identified in the CDA has been previously exploited.

Change # P1.07	Appendix D	Section 1.14	_
Proposed CSP Text **D1.14 AUTOMATED LABELING** **DELETED**			

Change # P1.08	Appendix D	Section 2.5	_

Proposed CSP Text

2.5 Response To Audit Processing Failures

This Technical cyber security **control manages responses to audit processing failures by performing the following**:

- **For CDAs that are part of centralized logging, if audit processing capabilities fail for a CDA or security boundary device, alerts are sent to designated officials.**
- **If the design configuration of the CDA's supports, provide a warning when allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity. The storage volume limit is based on the function of how quickly storage capacity is consumed and the organization's resources and response times.**
- **Actions are taken to preserve the audit logs for record retention requirements and after-the-fact investigations.**
- **Auditing failures will be assessed and determination of the device functionality should follow the CAP process.**
- **Justification and details for alternate compensating security controls are documented for those instances in which a CDA cannot respond to audit processing failures.**

Change # P1.09	Appendix D	Section 3.2	_

Proposed CSP Text

3.2 Application Partitioning/Security Function Isolation

This Technical cyber security control:

- Configures CDAs to separate applications into user functionality (including user interface services) and CDAs management functionality.
- Configures CDAs to isolate security functions from non-security functions. This is accomplished through partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform these security functions.
- **W**here a CDA cannot support security function isolation **implements alternative physical controls, such as**:
    - Physically restricts access to the CDA,
    - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
    - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
    - Ensures that individuals who have access to the CDA are qualified, and
    - Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.

Change # P1.10	Appendix D	Section 3.5	_
Proposed CSP Text **3.5 Resource Priority** **DELETED**			

Change # P1.11	Appendix D	Section 3.18	_
Proposed CSP Text **3.18 Thin Nodes** **DELETED**			

Change # P1.12	Appendix D	Section 3.20	_
Proposed CSP Text **3.20 Heterogeneity** **DELETED**			

Change # P1.13	Appendix D	Section 3.21	_
Proposed CSP Text **3.21 Fail In Known (Safe) State** **DELETED**			

Change # P1.14	Appendix D	Section 1.7	_

Proposed CSP Text

1.7 Unsuccessful Login Attempts

This Technical cyber security control:

- Implements security controls to limit the number of invalid access attempts by a user and documented this requirement in the access control policy. The number of failed user login attempts per specified time period may vary by CDA. For example, greater than three (3) invalid attempts within a one (1) hour time period automatically locks out the account. The system enforces the lock out mode automatically.
- Ensures that accounts can only be unlocked by authorized individuals who are not the locked out user when the maximum number of unsuccessful login attempts has been exceeded, and documents this requirement in the access control policy. Alternatively, use of other verification techniques or mechanisms which incorporate identity challenges may be used.
- Documents the justification and details for alternative controls/countermeasures where a CDA cannot support account/node locking or delayed login attempts **where CDAs do not support centralized logging:**
  - **Alternative controls/countermeasures are employed including: 24x7 monitoring, located in a Vital Area, located within a Locked Cabinet, or other physical control.**
- **Where** a CDA cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, alternative controls/countermeasures are employed to include:
  - Real time logging and recording of unsuccessful login attempts.
  - Real time alerting of designated personnel with the security expertise for the CDA through alarms when the number of defined consecutive invalid access attempts is exceeded.

Change # P1.15	Appendix D	Section 1.8	_

Proposed CSP Text

1.8 **System Use Notification**

This Technical cyber security control:

- **Where the design of the CDA supports the use of System Use Notification message and implementation does not have an adverse impact on the SSEP function;**
  - Displays a "System Use Notification" message before granting system access informing potential users:
    - That the user is accessing a restricted system.
    - That system usage may be monitored, recorded, and subject to audit.
    - That unauthorized use of CDAs is prohibited and subject to criminal and civil penalties, and
    - That the use of CDAs indicates consent to monitoring and recording.
  - Ensures that CDA "System Use Notification" message provides privacy and security notices.
  - Approves CDA "System Use Notification" message before its use.
  - Ensures that CDA "System Use Notification" message remains on the screen until the user takes explicit actions to log on to the CDA.
- Installs physical notices **at a central location to inform plant personnel of the potential consequences of unauthorized access to CDAs where System Use Notifications are not provided on the CDA.**

Change # P1.16	Appendix D	Section 1.9	_

Proposed CSP Text

1.9 Previous Logon Notification

This Technical cyber security control:

- **If the current design configuration of the CDA's operating system supports previous logon notification, then c**onfigures CDAs, upon successful logon, to display the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.
- Administratively requires end users to report any suspicious activity to the Cyber Security Program Manager.

Change # P1.17	Appendix D	Section 2.8	_

Proposed CSP Text

2.8 TIME STAMPS

This Technical cyber security control ensures CDAs use a time source protected at an equal or greater level than the CDAs or internal system clocks to generate time stamps for audit records, and the time on CDAs are synchronized.

The time of CDAs are synchronized from a dedicated source protected at an equal or greater level than the CDA existing on the security network, attached directly to the CDA, **via a GPS-based time server** or via SNTP and a trusted key management process.

Only methods of time synchronization that do not introduce a vulnerability to cyber attack and/or common-mode failure are utilized, or alternative controls are implemented to manage potential cyber security risks when time synchronization cannot be used for a CDA.

Change # P1.18	Appendix D	Section 1.2 and 2.2	_

Proposed CSP Text

1.2 Account Management

This Technical cyber security control:

- Manages and documents CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts.
- Reviews CDA accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on **temporary granted** CDA accounts at least every 31 days.
- **Licensee policies/procedures shall not allow temporary, guest, and emergency accounts unless their use is documented.**
- **Accounts on CDAs (Group or individual) shall only be authorized/terminated through station policies/procedures.**
- **Requiring access rights to be job function based.**
- **Any unauthorized accounts identified through an audit on a CDA will be documented in CAP for resolution.**

For CDAs that do not utilize Centralized Account Management

- **CDAs will use common role based group accounts to the extent possible. (Admin, User, Maintenance)**
- **Accounts will be used to enforce least privilege**
- **As a minimum, Accounts will be reviewed during maintenance/design activities where root/privileged level access is required.**
- **If individuals are granted unique access rights, then conduct reviews as individual's job function changes to ensure that rights remain limited to the individual's job function.**

For CDAs that use utilize Centralized Account Management

- **Accounts will be reviewed every 31 days.**
- **Conduct reviews when as individual's job function changes to ensure that rights remain limited to the individual's job function.**

2.2 Auditable Events [insert new bullet from D1.2 as last bullet in D 2.2]

- **Create and protect audit records for account creation, deletion and modification,**

Change # P1.19	Appendix E	Section 5	_

Proposed CSP Text

5 PHYSICAL PROTECTION

This family of security controls implements and documents physical protections for CDAs located outside the protected area. Physical protections for CDAs located inside the protected area are provided by the Physical Security Plan to comply with 10CFR73.55.

5.1 PHYSICAL PROTECTION POLICIES AND PROCEDURES

This security control develop**s**, implement**s**, review**s** in accordance with 10 CFR 73.55(m), and update**s**:

- A formal, documented physical protection policy that addresses:
  - The purpose of the physical security program as it relates to protecting the CDAs;
  - The scope of the physical security program as it applies to the organization's staff and third-party contractors;
  - The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with security policies and other regulatory commitments.

- Formal, documented procedures to facilitate the implementation of the physical protection policy and associated physical protection security controls.

5.2 THIRD PARTY/ESCORTED ACCESS

This security control consists of:

- Screening, enforcing and documenting security controls for third-party personnel and monitoring service provider behavior and compliance. Third-party providers include service contractors and other organizations providing control system operation and maintenance, development, IT services, outsourced applications, and network and security management.

- Including personnel security controls in acquisition-related contract and agreement documents.

5.3 PHYSICAL PROTECTION

This security control consists of securing and documenting physical access to CDAs. Physical security controls (e.g., physically isolate environment, locked doors, etc.) are employed to limit access to CDAs.

[Remainder of Section E.5 is unchanged.]

Change # P1.20	Appendix E	Section 8.5	_

Proposed CSP Text

8.5 CDA BACKUPS

This security control consists of:

- Conducting backups of user-level and system-level information.
- Backing up CDAs at an interval identified for the CDA or based on trigger events.
- Protecting backup information at the storage location.
- Testing and documenting backup information at an interval identified **in the licensee's procedures and justification is provided for the interval according to the licensee's assessment** to verify media reliability and information integrity.
- Using backup information in the restoration of CDAs functions as part of contingency plan testing.
- Protecting system backup information from unauthorized modification
- Storing backup copies of the operating system and other critical CDA software in a separate facility or in a fire-rated container that is not co-located with the operational software.
- Establishing and documenting the timeframe in which data or the CDA must be restored and the frequency at which critical data and configurations are changing.

END