Addendum 4 to NEI 08-09, Revision 6 Dated April 2010 Physical and Operational Environment Protection

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(b)(2) requires licensees to establish, implement, and maintain a cyber security program for the protection of the assets identified in 10 CFR 73.54(b)(1). Further, 10 CFR 73.54(c)(1) requires that the cyber security program must be designed to implement security controls to protect the assets identified in 10 CFR 73.54(b)(1) from cyber attacks

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. NEI 08-09, Appendices D and E provide cyber security controls to assist licensees in meeting the requirements in 10 CFR 73.54(c)(1).

Lessons learned through licensee implementation efforts, and through a series of implementation workshops conducted during 2016 that included industry and NRC observers indicate that clarification regarding acceptable approaches to implement certain cyber security controls is warranted. The clarifications 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 clarification to the cyber security controls documented in NEI 08-09, Revision 6, Appendix E, Section E.5, "Physical and Operational Environment Protection."

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. The guidance in this Addendum is applicable to any CDA, and incorporates tailored guidance for licensees that may have used NEI 13-10, "Cyber Security Control Assessments," to assist in implementation of cyber security controls.

1.4 USE OF THIS DOCUMENT

This document may be used to implement the Physical and Operational Environment cyber security controls.

1.5 ACRONYMS

The following acronyms are used in this document:

E.5 – Cyber security controls in Section 5 of Appendix E to NEI 08-09
PA – Protected Area
VA – Vital Area

2 PHYSICAL AND OPERATIONAL ENVIRONMENT PROTECTION GUIDANCE

This section provides guidance related to the Physical and Operational Environment Protection cyber security controls in Appendix E, Section E.5 of NEI 08-09, Revision 6.

2.1 GENERAL GUIDANCE

The NEI 08-09, Revision 6, Appendix E, Section E.5, "Physical and Operational Environment Protection," cyber security controls addressed in this guidance apply to Critical Digital Assets (CDAs), including those assessed under NEI 13-10 as both Direct and non-Direct and that are located outside of the Protected Area (PA) of nuclear power plant. As described in NEI 13-10 Section 5, "Baseline Cyber Security Protection Criteria," the E.5 controls are not required for Emergency Preparedness CDAs that have been assessed as having their function maintained by alternative means. However, if an EP CDA provides a pathway to a CDA(s) that would have an adverse impact to a safety or security function, this guidance shall apply.

The physical security controls in NEI 08-09, Appendix E, Section E.5, provide physical access control to delay and detect and respond to unauthorized physical access to CDAs which are located outside the PA. However, the E.5 controls are not meant to be equivalent to those required under 10 CFR 73.55 for physical protection of the PAs and Vital Areas (VAs) of a nuclear power plant. As a result, licensee corporate security or third party solutions may be used for addressing the E.5 controls.

For Direct and non-Direct CDAs outside the PA, the E.5 physical security controls are very important in addressing the technical security controls provided in licensee cyber security plans. Specifically, the physical security controls and physical isolation of non-Direct CDAs eliminate many of technical controls provided in the cyber security plan. Therefore, the intent of each of the security controls provided in E.5 needs to be met for CDAs to be maintained as non-Direct.

2.2 CYBER SECURITY CONTROL SPECIFIC GUIDANCE

The E.5 family of cyber security controls implements and documents physical protections for CDAs located outside the PA. Physical protections for CDAs located inside a PA or VA are provided by the Physical Security Plan to comply with 10 CFR 73.55.

This section reproduces the cyber security controls from NEI 08-09, and then provides implementation guidance.

2.2.1 Appendix E.5.1, Physical and Operational Environment Protection Policies and Procedures

Control language from NEI 08-09

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

- 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.

Guidance

This control applies to CDAs that are located outside the PA and VA.

2.2.2 Appendix E.5.2, Third Party/Escorted Access

Control language from NEI 08-09

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.

Guidance

One way to address the controls provided in E.5.2 is by using existing site physical security processes for PA (or other processes that are consistent with the physical security process for PA) that implement controls that meet the same security criteria for controlling the access by third parties or other personnel not cleared for unescorted access and screening and appropriately escorting when gaining access to locations with CDAs.

2.2.3 Appendix E.5.3, Physical & Environmental Protection

Control language from NEI 08-09

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).

Guidance

One way to address the controls provided in E.5.3 is by ensuring that CDAs are located in areas/facilities with robust walls, ceilings, and doors to prevent unauthorized access or entry. Locks, access control entry devices (i.e., key cards), or other means to ensure isolation and protection of CDAs should be implemented in a way that ensures positive control and appropriately facilitates assessment of unauthorized access. This control works in conjunction with the other E.5 controls to ensure protection, assessment and response to intrusions and should include the use of technologies such as tamper indicating devices and/or cameras or other means to assess the extent of an unauthorized entry into an area outside the PA with CDAs

2.2.4 Appendix E.5.4, Physical Access Authorizations

Control language from NEI 08-09

This security control consists of:

- Developing and maintaining a list of, and issuing authorization credentials (e.g., badges, identification cards, smart cards) to, personnel with authorized access to facilities containing CDAs and security boundary systems.
- Designating officials within the organization to review and approve the above access lists and authorization credentials, consistent with the access authorization program.

Guidance

One way to address the controls provided in E.5.4 is by using the existing site physical security processes for the PA (or other processes that are consistent with the physical security process for PA) that ensure personnel are screened and only authorized personnel are issued credentials that will allow access the areas with CDAs outside the PA. A designating official shall be identified and shall perform reviews and approval of access decisions and ensures that periodic reviews of authorized individual be often enough to ensure that the list remains current to protect the SSEP functions or Direct CDAs described in NEI 13-10 from cyber compromise of the CDAs by unauthorized individuals.

2.2.5 Appendix E.5.5, Physical Access Control

Control language from NEI 08-09

This security control consists of:

- Controlling physical access points (including designated entry/exit points) to locations where CDAs reside and verifies individual access authorization before granting access these areas.

- Approving individual access privileges and enforces physical and logical access restrictions associated with changes to CDAs.
- Controlling logical access through the use of electronic devices and software.
- Generating, retaining, and reviewing records pertaining to access restrictions.
- Ensuring qualified and authorized individuals obtain access to CDAs.
- Controlling physical access to the CDAs independent of the physical access controls for the facility.

Guidance

This control requires that access to CDAs are controlled through designated entry and exit locations and that measures are in place to verify current access authorization has been only granted in accordance with E.5.4 above. Third parties or individuals not authorized unescorted access must be processed and escorted in accordance with E.5.2.

Control of designated entry and exit points can be accomplished through the use of both manual and electronic methods. If employing manual means, such as door locks or padlocks, existing physical security key control program or other similar program must be in place to ensure only authorized personnel have access to keys, and measures must be in place to re-key locks upon loss of control of keys or changes of personnel with access to controlled keys.

If electronic devices and software, such as card readers are used to control entry, measures must be in place to detect attempts to tamper or bypass these systems. Logical access to these systems and software must be controlled and measures must be in place to ensure that only qualified individuals with authorized unescorted access can gain access to CDAs.

If CDA(s) are located in a facility that has access controls for a larger population of individuals that do not require or are not qualified for access to the CDAs, there must be additional barriers and access control to restrict access to CDA(s) to only those qualified, requiring access, and authorized IAWS Section 5.4 above.

CDAs in facilities or locations outside the control of the licensee, such as a switchyard owned by another company or part of the non-nuclear distribution division of a company, must be protected in accordance with this control.

However, for the BOP CDAs described in NEI 13-10, the physical access controls that are in place to meet North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards are sufficient to meet this requirement as long as:

- Formal agreements are in place to maintain these controls and only allow access to CDAs by personnel authorized by the licensee; and,

- The licensee security and other organizations are timely notified of potential tampering or attempted bypass, and any attempt to compromise a CDA through unauthorized access is detected and mitigated before adverse impact to safety or security function or Direct CDAs described in NEI 13-10.

For other locations outside the licensee's control, with no physical access control requirements, the licensee must ensure that adequate access control measures are in place for these CDAs to meet the objectives of the security controls provided in E.5.5. Physical locks or electronic means on the CDAs that are under the control of the licensee may be used to address this security controls by meeting the objectives of the security controls provided in E.5.5.

2.2.6 Appendix E.5.6, Access Control for Transmission Medium

Control language from NEI 08-09

This security control consists of controlling and documenting physical access to CDA communication paths.

Guidance

CDA transmission communications paths must be adequately controlled outside the PA to ensure that no unauthorized access or tampering has occurred. Underground cables must be placed in metallic or other similarly strong conduit material buried underground or imbedded in one foot of concrete to prevent the cable being dug up without being observed by OCA patrols, cameras or other means.

Access to cable that transitions a short distance from underground outside to the inside of secure buildings must be controlled by being run in metallic or other similarly strong conduit material, must not have un-monitored access panels, be hung aerially on poles, or be in open cable trays or under floors. Cabling conduit in this transition area must be subject to periodic and random observation at frequencies similar to that performed by the site OCA patrols or cameras.

Tamper indicating technology, assessment and response may also be used on transmission media systems to supplement protection if unable to satisfy some of the elements above.

2.2.7 Appendix E.5.7, Access Control for Display Medium

Control language from NEI 08-09

This security control consists of controlling and documenting physical access to CDAs that display information that may assist an adversary to prevent unauthorized individuals from observing the display output.

Guidance

Access to CDAs that display security sensitive information must be controlled in accordance with licensee processes and procedures for handling CDAs located inside the PAs to prevent the unintended and unauthorized disclosure of sensitive information through its visual presentation on a CDA-driven display. The scope of the sensitive information covered includes but is not

limited to security sensitive and SGI information, passwords or codes entered on a keypad, and other information that can assist in compromising the CDAs.

2.2.8 Appendix E.5.8, Monitoring Physical Access

Control language from NEI 08-09
This security control consists of:

- Monitoring and documenting physical access to CDAs and security boundaries to detect and respond to physical security incidents. For incidents, reviews physical access logs and coordinates results of reviews and investigations with the incident response personnel.
- Monitoring real-time physical intrusion alarms and surveillance equipment.
- Employing automated mechanisms to assess and recognize potential intrusions and initiates appropriate response actions.
- Providing lighting for access monitoring devices (e.g., cameras).

Guidance

Monitoring physical access, documenting and reviewing logs and alarms must be accomplished in accordance with existing or similar plant processes for the PA to meet the intent of the security controls provided in Section 2.2.7 (Appendix E.5.8, Access Control for Display Medium). A corporate level or third party monitoring capability may be used, but the licensee must also ensure that agreements are in place to:

- Monitor and document physical access to CDAs and security boundaries to detect and respond to physical security incidents. For incidents, reviews physical access logs and coordinates results of reviews and investigations with the incident response personnel.

- Monitor real-time physical intrusion alarms and surveillance equipment.

- Employ automated mechanisms to assess and recognize potential intrusions and initiates appropriate response actions.

- Provide lighting for access monitoring devices (e.g., cameras).

Use of surveillance equipment (e.g., cameras) with appropriate lighting, alarm monitoring, and response times must be commensurate with the CDA pathways and access to plant Safety and Security systems. For equipment that provides a pathway to systems or assets performing or supporting a safety or security function, real time monitoring and surveillance equipment is implemented to ensure assessment and prompt response to intrusions are commensurate with physical security response times to alarms associated with safety and security equipment inside the PA.

The following can be used for CDAs that are: considered isolated; are located in licensee access controlled facilities; do not have any pathways to other systems; are of limited functionality; and, whose compromise will have limited and easily quantifiable consequences:

- Use of identifiable tamper indicating devices that provide verification that no unauthorized access to the digital device has occurred;

- Performing periodic surveillance of tamper indicating devices; and

- Perform periodic functional and operational checks sufficiently often to ensure that the cyber compromise of the CDA can be detected in time to mitigate the compromise before adverse impact to safety or security functions or Direct CDAs described in NEI 13-10.

For Balance-of-Plant (BOP) CDAs, described in NEI 13-10, whose failure or cyber compromise could cause a reactor scram/trip, and that are located in facilities that are outside the PA or locations outside the control of the licensee, such as a switchyard owned by another company or part of the non-nuclear distribution division must have real time physical monitoring and surveillance in place by a corporate or third party provider and formal agreements to maintain these controls, restrict access to CDAs by unauthorized personnel, and allow timely licensee response to indications of tampering or bypass of the access controls to comply with NERC CIP Reliability Standards associated with monitoring physical access to these CDAs.

2.2.9 Appendix E.5.9, Visitor Control Access Records

Control language from NEI 08-09

This security control consists of:

- Controlling and documenting visitor physical access to CDAs by verifying the identity and confirming access authorization of these individuals prior to entry.
- Escorting visitors and monitoring visitor activity to prevent adverse impact to safety, security and emergency preparedness functions.

Guidance

Visitor control access records must be controlled in accordance with existing processes and procedures for the CDAs located inside the PAs or similar licensee processes and procedures.