Portable Media Scanning Stations / Kiosk Cyber Security Controls Evaluation Template

Prepared by the Nuclear Energy Institute
August 2018

The Nuclear Energy Institute is the nuclear energy industry's policy organization.
This document and additional about nuclear energy are available at nei.org
1201 F Street, NW Washington, DC 20004

REVISION TABLE

Revision	Description of Changes	Date Modified	Responsible Person
0	Initial Issuance	April 2018	R. Mogavero

NOTICE

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

The opinions, conclusions, and recommendations set forth in this report are those of the authors and do not necessarily represent the views of NEI, its employees, members or consultants.

Because NEI is supported in part by Federal funds, NEI's activities are subject to Title VI of the Civil Rights Act of 1964, which prohibits discrimination based on race, color, or national origin, and other federal laws and regulations, rules, and orders issued thereunder prohibiting discrimination. Written complaints of exclusion, denial of benefits or other discrimination of those bases under this program may be filed with the United States Nuclear Regulatory Commission, Washington, DC 20555 or any other appropriate federal regulatory agency or, among others, the Tennessee Valley Authority (TVA), Office of Equal Employment Opportunity, 400 West Summit Hill Drive, Knoxville, TN 37902

TABLE OF CONTENTS

1 INTRODUCTION

Kiosks, scanning stations, or scanning consoles (herein referred to as kiosks), if cyber compromised, could provide a possible Portable Media and Mobile Device (PMMD) attack pathway. Data and software is transferred to and from Critical Digital Assets (CDAs), through a kiosk, via passive media (e.g., CD) and/or active media (e.g., thumb drive or hard drive). When correctly performing their intended function, kiosks provide the main capability to detect known malware and ensure malicious data is not transferred to CDAs via the PMMD attack pathway. In many cases, licensees have not characterized these devices as CDAs. Physical and Cyber Security protection of the kiosk along with other cyber security controls that protect the CDA provide for mitigation of the PMMD pathway. Physical and cyber kiosk protections are needed to ensure that the kiosk is properly performing the transfer and detection functions as part of the protection of the PMMD pathway.

PMMD kiosks do not perform a plant Safety, Security or Emergency Preparedness (SSEP) function as defined by 10CFR73.54 (Reference 1). Further, the kiosks are not discussed in the accepted for use NEI 10-04 Revision 2 (Reference 4) and the generic Cyber Security Plan (CSP) provided in NEI 08-09 Revision 6 (Reference 3). This guidance has been developed to formalize the cyber security protection requirements for the kiosks to mitigate compromise and provide an additional layer of defense for the protection of CDAs.

This guidance is applicable to any kiosks, scanning stations or scanning consoles that are used by the licensee to scan portable media and other scannable digital equipment used on CDAs and for data transfers to and from CDAs.

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 licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks. 10 CFR 73.54 (a) (2) specifically requires that *"licensee shall protect the systems and networks identified in paragraph (a) (1) of this section from cyberattacks that would:*

> *(i) Adversely impact the integrity or confidentiality of data and/or software; and*
>
> *[…]*
>
> *(iii) Adversely impact the operation of systems, networks, and associated equipment."*

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, Appendix D 1.19 "Access Control for Portable Media and Mobile Devices" specifically requires that licensees:

- Establish and document usage restrictions and implementation guidance for controlled portable and mobile devices.
- Authorize, monitor, and control device access to CDAs.
- Enforce and document mobile device security and integrity are maintained at a level consistent with the CDA they support.

- Enforce and document mobile devices are used in one security level and mobile devices are not moved between security levels.

Security Frequently Asked Questions (SFAQ) 16-05, "Moving Data between Security Levels," provides additional guidance for transferring data and software to and from CDAs and for protecting PMMD scanning stations and kiosks. SFAQ 16-05 clarifies requirements identified in NRC Enforcement Memorandum "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for 'Good-Faith' Attempt Discretion." This guidance can be used to define cyber security controls to protect the kiosk functions of detection and data transfer. SFAQ 16-05 specifically addresses PMMD Kiosk Security Control Protection, stating:

> *Additional security controls to harden and maintain PMMD scanning stations/kiosks can help ensure that PMMD scanning stations/kiosks do not reduce the established cyber security assurance levels of the CDAs they service. The Enforcement Memorandum also states that the attack vectors introduced by the scanning stations/kiosks should be mitigated, the stations hardened and maintained, and external network connections to the stations eliminated. In order to harden and maintain scanning/transfer stations, licensees should perform and document analyses to address the guidance in NEI 08-09, Rev. 6 Appendix D5 technical cyber security controls:*
>
> - *D5.1 (Removal of Unnecessary Services and Programs)*
> - *D5.3 (Changes to File System and Operating System Permissions)*
> - *D5.4 (Hardware Configuration)*
> - *D5.5 (Installing Operating System, Applications and Third-Party Software Updates)*
>
> *The PMMD scanning station/kiosk should have more than one virus scanning engine (or whitelisting), one of which includes heuristic scanning. The PMMD scanning station/kiosk should also utilize countermeasures (e.g., a white-listing software product, access control, account management, configuration management) as required to protect the kiosk integrity. In order to facilitate monitoring and maintenance, it may be acceptable to configure multiple scanning stations/kiosks with a management console in an air-gapped network.*

SFAQ 16-05 was developed to provide guidance to meet the requirements of the Enforcement Memorandum and implementation of Milestone 4. SFAQ 16-05 goes on to state that, "[f]or full implementation, controls may need to be implemented to ensure that PMMD scanning stations/kiosks and the management console do not reduce the established cyber security assurance levels of the CDAs that they service."

Clarifications to terms used in the SFAQ and this guidance document:

1. The term "whitelisting" as first used in the SFAQ refers to a user-defined list of acceptable file types and sources (and possibly specific names) that are permitted to be scanned and passed through the kiosk. This type of whitelisting is more commonly referred to as Application Whitelisting.

2. The term “white-listing” as used subsequently in the SFAQ refers to the installation of a third party application that controls what programs/processes are permitted to be executed by the native operating system (e.g., MS Windows or Linux) of the kiosk. White-listing functions may be included in the operating system and are often bundled in many products referred to as End-Point-Protection applications that provide Host Intrusion Detection (HID), Host Intrusion Prevention (HIP), Anti-Virus Scanning, Device Control (e.g., USB, Serial Port and Ethernet device authorization) and Application Whitelisting. This cyber security software would be a key defense in depth element that prevents the execution of malware on the kiosk as required in the SFAQ.

3. The term “air-gapped” network as used in the SFAQ is intended to mean a LAN containing kiosks and a management console, but having no other connectivity. In this guidance document the term “isolated network” means dedicated network that is logically segmented to prevent bi-directional information flow with another network of a lower defensive level (e.g., using a data-diode) for the purpose of obtaining out-going alerts, alarms and logs. The term “interconnecting-LAN” is used to mean either an air-gapped or isolated LAN.

4. The term “management console” as used in the SFAQ refers to a computer that is either permanently or periodically connected to an air-gapped or isolated LAN for the purpose of administrative management and maintenance of the kiosks.

This guidance is developed to ensure protection of kiosks and to support NRC oversight activities to ensure consistency in inspections.

This document is intended to clarify what is required for full program implementation of the kiosk in support of the PMMD program. This document will guide the licensee in completing an evaluation that determines the necessary controls for addressing the five threat vectors and securing the kiosk from being used as part of an attack pathway to CDAs. The guidance in this document is intended to add necessary clarity and, if implemented, does not decrease the effectiveness of cyber security plans implemented using the guidance in NEI 08-09, Revision 6. Licensees continue to have the capability, under NEI 08-09, Revision 6, Appendix A Section 3.1.6, to implement alternate approaches to what is described in this document.

1.2 Purpose

This guidance document provides a standard evaluation format, control guidance and implementation strategies to provide protection of kiosks in order to secure the kiosk from being used as part of an attack pathway to CDAs. The controls identified ensure that kiosks and the management console do not reduce the established cyber security assurance levels of the CDAs that they service. Physical and cyber security protection of the kiosk along with other cyber security controls that protect the CDA provide for mitigation of the PMMD pathway. Physical and cyber security kiosk protections are needed to ensure that the kiosk is properly performing the transfer and detection functions as part of the protection of the PMMD pathway.

1.3 Scope / Approach

The guidance in this document is applicable to power reactor licensees with Cyber Security Plans (CSP) based on the template in NEI 08-09, Revision 6. Attachment 1 provides a template/method to evaluate

kiosks against the cyber security controls of NEI 08-09, Revision 6 (as determined to be applicable within this guidance).

This guidance evaluates applicability of cyber security controls, as defined in NEI 08-09, Revision 6 for kiosks. Cyber security controls are applied to the kiosks based on meeting the following criteria:

1. Cyber security controls provide protection of the kiosks, and to any inter-connecting isolated LAN and management console, to ensure the kiosk functions of known malware and corrupted software detection and data transfer are protected.

2. When an evaluation of the kiosk configuration/implementation determines that the threat vectors have not been fully mitigated, the controls listed in Section 3 and Attachment 1 of this document are to be addressed using CSP Appendix A Section 3.1.6 including NEI 08-09, Revision 6, Addendum 1 (Reference 6).

3. Vendor kiosk product recommended controls are addressed.

This evaluation does not provide a detailed evaluation of all controls and sub-controls of NEI 08-09, Revision 6. If the control would not provide "enhanced protection" of the kiosks then the control was not considered.

1.4 Use of This Document

This document may be used to implement the cyber security protection of kiosks and any associated isolated-LAN and management console.

Attachment 1 provides a template to address the NEI 08-09, Appendices D & E selected controls for kiosk function protection. A site-specific kiosk evaluation should be developed to analyze kiosk protection. The site-specific analysis should document:

1. Implementing the cyber security controls in Attachment 1 for kiosks and management work stations.

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 provided in Attachment 1 by:

    a. Documenting the basis for employing alternative countermeasures;

    b. Performing and documenting the analyses of the kiosk and alternative countermeasures to confirm that the countermeasures mitigate the consequences of the threat/attack vector the control is intended to protect against;

    c. Implementing alternative countermeasures determined in item (b); and

    d. Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate.

3. Not implementing one or more of the cyber security controls by:

a. Performing an analysis of the specific cyber security controls for the kiosk 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.

1.5 Definitions

Cyber Security Vulnerability – A feature, attribute or weakness in a system's design, implementation or operation and management that could render a CDA open to exploitation or SSEP function susceptible to adverse impact.

Logical Access Control – A design feature of a digital asset that controls the ability to access resources and/by information. This may include requiring a form of user identification and/or authentication via a human-machine interaction. Logical access controls can range from simple authentication (e.g., entering a 4-digit passcode) to more complex multi-factor authentication (e.g., something they know (i.e., a password), possess (i.e., an access card) or are (i.e., biometrics)).

Logging – Automatically created network device, operating system or application files containing time/date 'tagged' and chronologically ordered records of designated activities. Logs are intended to document user and device activity to support after-the-fact analyses associated with incidents and events. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity and operational problems.

(Kiosk) Management Console – A computing device that is permanently or occasionally attached to an isolated-LAN to which multiple scanning stations/kiosks are also connected and which is used to provide log collection or review, centralized configuration management, signature/rule updating, patching and software updating of the scanning stations/kiosks.

Scan Station – A computing device (e.g., laptop, custom purpose-built system, dedicated PC, etc.) featuring multiple types of specialized malware detection software designed to scan portable media using a CDA's compatible file format for malware identification. The malware detection software includes heuristic analysis functionality to help identify previously unknown computer viruses.

Scanning Kiosk – A free-standing or isolated/air-gapped LAN-connected terminal featuring multiple types of specialized malware detection software designed to scan portable media using any Windows compatible file format (e.g., FAT32 or NTFS). The malware detection software includes heuristic analysis functionality to help identify previously unknown computer viruses. Both scanning and file transfers are performed using a kiosk.

2 KIOSK PROTECTION AND CONTROLS APPLICABILITY

2.1 General Guidance

PMMD kiosks do not perform a plant Safety, Security or Emergency Preparedness (SSEP) function as defined by 10CFR73.54 and are also not discussed in NEI 10-04; NEI 08-09, Revision 6 (accepted for use by the NRC); or in the licensee CSP.

However, they are part of the site PMMD attack pathway mitigation strategy, and as a result, must be protected against cyber compromise at a level commensurate with the CDAs they support in order to have assurance that they operate as required to protect CDAs. Evaluation, application and documentation of appropriate controls should be applied to kiosks, and to any applicable management consoles and interconnecting LAN, to protect the PMMD attack pathway. The following cyber security control guidance should be applied to kiosks. This guidance was developed using the guidance defined in NEI 08-09, Revision 6, and Addenda 1-5.

2.2 Attack Pathway and Attack Vector discussion

This guidance document provides recommended controls to mitigate the kiosk attack pathways. A summary of the potential attack pathways and mitigating features is provided in this section. Implementation of applicable cyber security controls identified in Section 3 and Attachment 1 provides high assurance that risk of a potential cyberattack on the kiosk, via kiosk attack pathways (plus interconnecting-LAN and management console pathways, if applicable) has been mitigated.

Cyber security controls are not applied if the control adversely impacts the kiosk function. When a cyber security control is determined to have an adverse effect, alternate controls are used to mitigate the lack of the security control for the kiosk per the process described in Section 3.1.6 of the CSP.

Detailed procedures cover the PMMD program and procedure compliance has a high level of assurance through implementation of several layers of regulatory-based administrative controls and programs at a Nuclear Power Plant. These programs and controls include an accredited training and qualification program, the Insider Mitigation Program required by 10CFR73.56, station policy on procedure use and adherence to comply with the licensing basis, commitments on procedures, and supervisory and management oversight.

To determine what cyber security protections are necessary, an analysis of the potential attack vectors is performed. The resulting vector mitigation strategies define the cyber security controls necessary to protect the kiosk detection and data transfer functions. An attack vector exists if the adversary has access to any of the following attack pathways:

- Physical access to the kiosk
- Wired network connection to the kiosk (if on an interconnecting-LAN)
- Wireless network connection to the kiosk
- Portable Media and Mobile Devices (PMMD) connection to the kiosk (and management console, if applicable)
- Supply chain access

A description of the mitigation attack pathway and attack vector for kiosks is provided below.

Mitigation of the Physical Security Attack Pathway

Compromise of the kiosk programming (e.g., operating software and scanning engines) is possible if an attacker gains physical access to the kiosk data ports or digital hardware.

For kiosks located within the Protected Area (PA), the requirements of 10CFR73.55 and 10CFR73.56 and the site's Physical Security program, Access Authorization programs and additional controls of the kiosk provide high assurance of protection from a physical threat vector involving an unauthorized individual. Physical controls include the implementation of the unescorted access/site access program, visitor access program and continuous physical security systems monitoring. Access to the kiosk internal components should be restricted through the use of a locked enclosure and physical key control program, or the detection of unauthorized access through the use of tamper-indicating devices.

For kiosks located outside the Protected Area (PA), the Physical Environment Protection controls of NEI 08-09, Revision 6, Appendix E.5 and Addendum 4 identify the security controls to provide high assurance of protection from a physical threat vector involving an unauthorized individual. Access to the kiosk internal components should be restricted through the use of a locked enclosure and physical key control program or the detection of unauthorized access through the use of tamper indicating devices.

Kiosks (as well as management consoles) are also protected with access controls (e.g., administrative user login, accounts and passwords) to provide logical security protection. Access to and manipulation of kiosks (and any management consoles) are performed by qualified station personal and controlled by station procedures/policies.

Implementation of the cyber security controls identified in Section 3 and Attachment 1 of this document provides assurance that the physical security attack pathway has been mitigated.

Mitigation of the Wired Network Attack Pathway

Compromise of the kiosk programming (e.g., operating software and scanning engines) is possible if an attacker gains logical access to the kiosk data ports or digital hardware through a wired connection.

Kiosks can be either standalone devices, or connected to an interconnecting LAN, which itself is either fully air-gapped or deterministically protected from cyberattacks initiated from other networks, which provides high assurance of protection from a network attack. A network attack requiring physical access has been mitigated through the Physical Threat Vector Analysis (see mitigation measures under Physical Threat Vector Analysis). If the interconnecting LAN, if applicable, also includes a management console, then that console must be given adequate cyber protections (the necessary controls applied) so that it cannot be used as an attack platform from which to cyber compromise the kiosks.

Implementation of the cyber security controls identified in Section 3 and Attachment 1 of this document, on the kiosks and management console, provides assurance that the wired network attack pathway has been mitigated.

Mitigation of the Wireless Network Attack Pathway

Compromise of the kiosk programming (e.g., operating software and scanning engines) is possible if an attacker gains logical access to the kiosk data ports or digital hardware through a wireless connection.

Kiosks wireless capability (and management console, if applicable) is disabled following the guidance in Section 3 and Attachment 1. The use of wireless technologies for kiosks and management consoles are prohibited. Wireless router/access-points are prohibited from being connected to the interconnecting LAN containing kiosk and management consoles.

Implementation of the cyber security controls identified in Section 3 and Attachment 1 provides assurance that the wireless network attack pathway has been mitigated.

Mitigation of the Portable Media Attack Pathway

Compromise of the kiosk programming (e.g., operating software and scanning engines) is possible if an attacker gains logical access to the kiosk data ports or digital hardware through the PMMD connection.

The kiosk function is to protect PMMD and information flow to CDAs. The licensee PMMD program implemented in accordance with NEI 08-09, Revision 6 and SFAQ 16-05 along with the hardening and additional cyber security controls identified in Section 3 and Attachment 1 of this document ensure that the PMMD attack pathway is mitigated.

Mitigation of the Supply Chain Pathway

Compromise of the kiosk programming (e.g., operating software and scanning engines) is possible if an attacker gains logical access to the kiosk data ports or digital hardware through the supply chain connection prior to installation testing at the nuclear power plant.

Kiosks are protected from the supply chain pathway by testing for vulnerabilities and the use of effective security controls prior to introduction into a production environment or network, as well as throughout the system's lifecycle. Licensee testing should be performed in accordance with NEI 08-09, Revision 6, Appendix E11 and the guidance of Addendum 3 to NEI 08-09, Revision 6 as provided in Attachment 1.

3 KIOSK CYBER SECURITY EVALUATION TEMPLATE

A standard industry approach to evaluating kiosks and scanning stations has been developed and provided in Attachment 1. This evaluation template incorporates the guidance provided above and provides a cross-reference to the NEI 08-09, Revision 6, Addendum 1 Cyber Security Controls. Each licensee will differ to some degree based on architecture, policies and procedures, implementation of controls and software employed.

4 REFERENCES

1. 10CFR73.54, Protection of digital computer and communication systems and networks.

2. NEI 08-09, Revision 6, Addendum 1, "Cyber Security Plan for Nuclear Power Reactors," Dated March 2017.

3. NEI 13-10, Revision 6, "Cyber Security Control Assessments," Dated August 2017.

4. NEI 10-04, Revision 2, "Identifying Systems and Assets Subject to the Cyber Security Rule," Dated July 2012.

5. Security Frequently Asked Questions (SFAQ) 16-05, “Moving Data between Security Levels,” Dated February 28, 2011 (Agency wide Documents Access and Management System (ADAMS), Accession No. ML110600211).

6. Addendum 1 to NEI 08-09, Revision 6, “Change Descriptions and Justifications,” Dated March 2017.

7. Addendum 2 to NEI 08-09, Revision 6, “Cyber Attack Detection, Response and Elimination,” Dated July 2017.

8. Addendum 3 to NEI 08-09, Revision 6, “System and Services Acquisition,” Dated August 2017.

9. Addendum 4 to NEI 08-09, Revision 6, “Physical and Operational Environment Protection,” Dated July 2017.

10. Addendum 5 to NEI 08-09, Revision 6, “Cyber Security Vulnerability and Risk Management,” Dated July 2018.

11. Good Faith Letter, "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good-Faith" Attempt Discretion,” Dated July 1, 2013.

ATTACHMENT 1: KIOSK CYBER SECURITY CONTROLS

Control	Control Title	Stand-alone	Networked	Program	Guidance
Appendix D1 Access Controls					
D1.1	Access Control Policies and Procedures	X	X	X	A formal, documented kiosk access control policy is developed, disseminated, reviewed and updated as required.
D1.2	Account Management	X	X		Access Control Rights (e.g., administrator rights) on the kiosk (and management console, if applicable) are limited to Cyber Security Staff as authorized by the CSPM. There should be at least two types of accounts: USER accounts with limited access rights that do not allow any changes to be made to the kiosk but allow normal users to scan and transfer data from one PMMD to another; and ADMINISTRATOR accounts that have administrator access to make changes to the kiosk operating system and configuration. ADMINISTRATOR accounts are not to be used for normal kiosk use. Apply password protection (administrative, BIOS and upon reboot) to limit authorized access (refer to required D4.3 controls in this document for password requirements). Reviews should be conducted when individuals' job function changes to ensure that rights remain limited to those that continue to require administrative access.
D1.3	Access Enforcement	X	X		Restrict access to administrative functions (deployed in hardware, software and firmware) and security-relevant information to authorized personnel. Employ key controls on the kiosks or other equivalent means to restrict physical and administrative access to the device for other than scanning and data transfer. For those kiosks and management consoles located within the PA the physical restrictions and protection controls are adequate to meet the physical security controls for scanning and data transfer. For kiosks or management consoles located outside the PA refer to E5 controls in this document for physical protection requirements for kiosks and management consoles outside the PA.
D1.4	Information Flow Enforcement		X		Kiosks have no need to intercommunicate and do not exchange data except when being maintained and administered via a LAN-connected management console. Only the TCP and UDP ports used for cross-LAN administration will be unblocked on the kiosks and management consoles, restricting unauthorized information flows between kiosks. Scanning kiosks that perform file transfers must implement this control by controlling the flow of data within the kiosk to assure that no unauthorized data or information is passed to any other system. Effective implementation of this control by the kiosk provides a secure pathway of data transfer within the kiosk and ensures that data stored on the trusted media will comply with the licensee's security policy for the CDA. LAN-connected kiosk systems will have no connection to external systems or networks, except via a deterministic device. This prevents unauthorized information flows from being externally initiated.
D1.5	Separation of Functions	X	X		There are two modes of operation: non-administrators will log into the kiosk with "USER mode" which only allows the user to scan and copy PMMD. When administrators log in, they are given "ADMINISTRATIVE access" which allows them to update the files on the kiosk.

Control	Control Title	Stand-alone	Networked	Program	Guidance
D1.6	Least Privilege	X	X		Administrative support of the kiosks and, if applicable, management consoles, requires full-access ADMINISTRATIVE accounts be assigned to authorized and trained personnel. USER accounts will have restricted limited-rights access. Consider using service accounts with limited rights, where applicable, which would not require a login.
D1.7	Unsuccessful log in attempts	X	X		Implement security controls to limit the number of invalid access attempts to the administrative account by an admin user. The number of failed user login attempts (maximum of 5) per specified time is implemented to ensure automatic lock out of the account for a minimum of 30 minutes. If unable to limit the number of invalid access attempts or automatically lockout access for a minimum of 30 minutes due to kiosk design, alternate controls include physically restricting access to the kiosk and implementing access controls (e.g., key control or electronic key card access).
D1.8	System Use Notification				N/A
D1.9	Previous Logon Notification				N/A
D1.10	Session Lock	X	X		If unable to limit the number of invalid access attempts or automatically lockout access for a minimum of 30 minutes due to kiosk design, alternate controls include physically restricting access to the kiosk and implementing access controls (e.g., key control or electronic key card access).
D1.11	Supervision and Review	X	X		Documents, supervises and reviews the activities of users with respect to the enforcement and usage of access controls every 14 days. This can be satisfied by periodic review of security logs for other controls. Provides supervisor approval/authorization of work orders and plans for performing updates/management of kiosks and management consoles. May employ automated mechanisms within kiosks to support and facilitate the review of user activities.
D1.12	Permitted Actions without Identification or Authentication				N/A
D1.13	Automated Marking				N/A
D1.14	Automated Labeling				N/A
D1.15	Network Access Control		X		For networked kiosks, establish network access control by configuring the “port security” functionality (MAC address lists) on the Ethernet switches that form the isolated LAN in order to block unauthorized devices from gaining network access. Unused switch ports will be administratively disabled or physically blocked. Administrative access to Ethernet switches will be password restricted.
D1.16	Open/Insecure protocol		X		Avoid insecure protocols for communications between the kiosks and management consoles unless they are required and secure alternatives are not available (e.g., on devices where ssh and https can be used in place of telnet and http insecure protocols are to be disabled). As there are no “users” and no centralized user authentication mechanism there will be no cross-network insecure message traffic that could disclose user credentials.
D1.17	Wireless Access Restrictions	X	X		Disable wireless capabilities (Wi-Fi and Bluetooth) on kiosks and management consoles. Rogue wireless scans are not required as long as the following controls are implemented: • Wireless capability is disabled, and • Kiosks/scanning stations are hardened in accordance with D5 controls, and • Location is physically protected (either within the PA or E5 controls are applied)

Control	Control Title	Stand-alone	Networked	Program	Guidance
D1.18	Insecure and Rogue Connections	X	X		All exposed interfaces should be restricted to the scanning and data transfer functions and/or forensic information. Networked kiosks should restrict the removal of, or apply tamper indicators, to any LAN connection and block all unused communications ports. Implementing D5 controls and physical protection controls meet this requirement. Kiosks will be examined for rogue connections each time internal access is needed for maintenance or support purposes. Management consoles will be inspected for rogue connections at least every 31 days. Effective alternate countermeasures to performing insecure connection inspections include: • Kiosk (and any associated network and management consoles) is entirely within a vital area • Kiosk (and any associated network and management consoles) is entirely within a protected area, and any devices locked and key-controlled (room, cabinet, etc.) • If the kiosk (and any associated network and management console) is located within the OCA an effective alternate countermeasure includes: o Protection in accordance with E5 controls, and o Hardening controls in accordance with D5, and wireless is disabled in accordance with D1.17 controls, and o Application Whitelisting is applied, and o Kiosks are network connected with technology capable of detecting insecure and rogue connections (e.g., NIDS using a deterministic one-way network tap or topology monitoring software).
D 1.19	Access Control for Portable Media and Mobile Devices	X	X		Ensures that individuals who have access to the devices are qualified in accordance with the licensee's PMMD program. D1.19 Access Control for Portable Media and Mobile Devices (PMMD) will be implemented in accordance with licensee PMMD program for portable media and mobile devices used to maintain, support and administer the kiosks and management console.
D 1.20	Proprietary protocol		X		This control is only applicable to kiosks that are connected to a vendor-proprietary network or connected to an IP/Ethernet-based network and utilize proprietary protocols. If the kiosk does not support network connectivity or only IP/Ethernet connectivity, and uses only well-known protocols, then the attack vector does not exist and the control is not applicable. The kiosks and management consoles do not make use of any vendor-proprietary protocols.
D 1.21	Third Party Products and Controls	X	X		This control is only applicable to kiosks that fall under contractual agreements that prohibit making software changes or installing 3rd-party software. If a kiosk has no such prohibitions then the control is not applicable. If a kiosk has such prohibitions, alternate countermeasures may be required.
D1.22	Use of External Systems		X		This control would only be applicable to kiosks that are network connected. The interconnecting LAN to which the kiosks and management consoles are attached is either isolated (air-gapped) or only connected to external systems using a deterministic device. In either case communication interaction is not possible with external systems and thus the control is not applicable.
D1.23	Public Access Protections				N/A
Appendix D2 Audit and Accountability					
D2.1	Audit and Accountability Policy	X	X	X	Controls should be implemented in accordance with the licensee audit and accountability policy.

Control	Control Title	Stand-alone	Networked	Program	Guidance
D2.2	Auditable Events	X	X		Auditable events include administrative login/logouts, configuration/software/firmware changes, setting changes, privileged/administrative access, privileged commands, and any modifications of the security functions of kiosks or management consoles. The security event logs of the operating systems of the kiosks and management consoles include the specified information and will be enabled on the kiosks and management consoles. Prevents kiosks from purging audit event records on restart unless the kiosks are sending their logs via Syslog messages to either the SIEM or a management console (in which case a backup is being maintained.)
D2.3	Content of Audit Records	X	X		Ensures that kiosks produce audit records that contain sufficient information to establish what events occurred, when the events occurred, where the events occurred, the sources of the events, and the outcome of the events. The security event logs of the kiosk and management consoles regularly collect and include this kind of information.
D2.4	Audit Storage Capacity	X	X		Allocates sufficient audit record storage capacity to ensure records are available until reviewed. For LAN-connected kiosks with a permanent management console the management console can be configured as a Syslog server to receive, consolidate and store logs from all of the kiosks as a backup. If logs are to be periodically manually transferred to a SIEM this log consolidation will eliminate the need to individually collect logs from each of the kiosks. If there is a pathway to send logs to the SIEM (e.g., via a data-diode connection) then the SIEM will provide the required storage capacity.
D2.5	Response to Audit Process Failures	X	X		Ensure kiosks provide a warning when allocated audit record storage volume reaches a defined percentage of maximum audit record storage capacity, and ensure organizational response. In a LAN-connected configuration with a permanent management console, if there is no pathway for sending logs to the plant-wide SIEM, the individual kiosks can also forward their logs to the management console (using Syslog protocol) as a redundant storage site. If logs are being sent to the SIEM then the SIEM itself provides log storage backup.
D2.6	Audit Review, Analysis and Reporting	X	X		Unless the logs are being forwarded to the SIEM, review and analyze the kiosk audit records at least every 14 days, for indications of inappropriate or unusual activity, and report the findings to the designated official. If LAN-connected kiosks forward their logs to the permanent management console, but not to the SIEM, then only the aggregated logs on the management console need to be reviewed every 14 days. For networked kiosks that include near real-time monitoring capability to identify and detect potential compromise log reviews are not required every 14 days.
D 2.7	Audit Reduction and Report Generation	X	X		For kiosks connected to a SIEM, provide kiosk audit report generation capability by integrating the kiosk logs into the plant-wide SIEM and using the SIEM's report generation capabilities. For kiosks not connected to a SIEM, manual review of audit logs is acceptable. In this case, provide documentation identifying which logs are reviewed and the type of events that are being examined.
D2.8	Time Stamps	X	X		Networked kiosks providing event logging information to a SIEM or management console shall have their time clocks synchronized. Standalone kiosks whose event logs are manually transferred to a SIEM shall have their time clocks' accuracy checked and or reset after transferring logs.
D2.9	Protection of Audit Information	X	X	X	This should be implemented IAW licensee CSP.
D2.10	Non-repudiation	X	X	X	This should be implemented IAW licensee work control procedures for removing and reviewing audit logs.
D2.11	Audit Record Retention				N/A
D2.12	Audit Generation				N/A
Appendix D3 CDA, System and Communications Protection					
D3	CDA, System and Communications Protection				This entire section is N/A

Control	Control Title	Stand-alone	Networked	Program	Guidance
Appendix D4 Identification and Authentication					
D4.1	Identification and Authentication Policies and Procedures	X	X	X	Completion and approval of a kiosk control guidance document in accordance with this document will serve as the access control policy for kiosks.
D4.2	User Identification and Authentication	X	X		Access Control Rights (e.g., administrator rights) are limited to Cyber Security Staff as authorized by the Cyber Security Program Manager. Ensure that individuals who have access to the devices are qualified, and ensure that those individuals are trustworthy and reliable per 10CFR73.56. Physical access restriction to the kiosk is provided in accordance with applicable App E5 controls for those kiosks located outside the PA.
D4.3	Password Requirements	X	X		Applies administrative, reboot and BIOS passwords to kiosks. Password authentication is required upon reboot of the device. Passwords are changed and controlled in accordance with licensee password policy. Length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the kiosk.
D4.4	Non-Authenticated Human Machine Interaction (HMI) Security				N/A
D4.5	Device Identification and Authentication	X	X		Implements and documents technology that identifies and authenticates devices (such as device whitelisting) before those devices establish connections to the kiosk or management console. Implements alternative controls/countermeasures where a kiosk or management console cannot support device identification and authentication (e.g., serial devices) and implements the following: • Physically restricts access to the management consoles, • Maintain and control use of kiosk enclosure keys, • Monitors and records physical access to the kiosks and management consoles 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 kiosks and management consoles, Ensures that individuals who have internal physical and logical administrative access to the kiosks and management consoles are qualified, and ensures that those individuals are trustworthy and reliable per 10CFR73.56.
D4.6	Identifier Management				N/A
D4.7	Authenticator Management				N/A
D4.8	Authentication Feedback	X	X		Ensures that kiosks and management consoles obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Ensures that feedback from kiosks and management consoles do not provide information that would allow an unauthorized user to compromise the authentication mechanism.
D4.9	Cryptographic Module Authentication				N/A
Appendix D5 System Hardening					

Control	Control Title	Stand-alone	Networked	Program	Guidance
D5.1	Removal of Unnecessary Services and Programs	X	X		Document all applications, utilities, system services, scripts, configuration files, databases, and other software and the appropriate configurations, including revisions and/or patch levels for the kiosks and management consoles. Verify and document that kiosks and management consoles are patched or mitigated in accordance with the patch management process and security prioritization timelines according to NEI 08-09, Revision 6, Appendix E, Section 3.2, Flaw Remediation. Remove unnecessary programs and disable unnecessary services not intrinsic to the normal operation of the kiosk. Vendor recommendations should be consulted when disabling services to avoid any discontinuity of operations or impairment of the kiosk functions.
D5.2	Host Intrusion Detection System	X	X		Virus scanning of the OS file system and program memory shall be periodically applied to kiosks and management consoles. These malware scans should use more than one virus scanning engine, one of which will include heuristic scanning, with virus definitions updated in accordance with vendor recommendations, but not less frequently than once every 14 days. Application whitelisting, which is a highly effective form of HIDS technology, should be installed on each kiosk and management console and the associated logs forwarded to the SIEM if possible, or periodically reviewed manually. Physical protection of the kiosks and management consoles will be provided in accordance with Section 2.2.1. To further enhance the kiosk security one of the following must be implemented: • Kiosk is SIEM connected and monitored, or • Automated kiosk application software lockout to prevent its use when a security event occurs within the kiosk OS when technically feasible, or • Review security logs (including the whitelisting application logs) every 14 days, unless logs are being sent to the SIEM, and before placing the kiosk back in service after each repair or inoperative state, or • Verification testing per one of the following methods: o Verification of file hash signatures before and after the scanning process, or o Functionally tested (e.g., test that verifies that signatures are functioning, such as the use of a benign virus signature file). If application whitelisting is not utilized on kiosks and management consoles then additional review of NEI 08-09, Revision 6 controls may be required to ensure equivalent protection. Other means maybe appropriate to provide timely detection and should be documented within the license's evaluation and cyber security program.
D5.3	Changes to File System and Operating System Permissions	X	X		Configure kiosks and management consoles such that only administrator accounts can make changes to the file system and operating system permissions. Have the kiosk system vendor configure the system services to execute at the least privilege level possible and to document the configuration. Validate baseline permission and security settings are not altered after modifications or upgrades.

Control	Control Title	Stand-alone	Networked	Program	Guidance
D5.4	Hardware Configuration	X	X		Disable through software or physical disconnection, or the use of engineered barriers, interfaces, communication ports and removable media drives for any of these not required for the scanning and data transfer function of the kiosks. Disable through software or physical disconnection, or the use of engineered barriers, interfaces, communication ports and removable media drives for any of these not required for the functions of the management consoles. Password protects the BIOS from unauthorized changes. Document the hardware configuration (disabled or removed USB ports, CD/DVD drives, and other removable media devices). Allow system administrators the ability to re-enable devices if the devices are disabled by software and document the configuration. Verify that replacement devices are configured equal to or better than the original.
D5.5	Installing Operating Systems, Applications, and Third Part Software Updates	X	X		Document the patch management program, update process, and individuals responsible for installation. Document notification of vulnerabilities affecting kiosks to be conducted within the maximum periodicity defined in the risk determination. Document notification to authorized personnel of patches affecting cyber security. Tests updates on a non-production system for testing and validation prior to installing on production systems when practical.
Appendix E1 Media Protection					
E1.1	Media Protection Policy and Procedures (SGI, Non-SGI and 2.390)	X	X	X	For licensees that utilize kiosks or scanning station for sanitization: For SGI and SRI information, the licensee's information protection is addressed by site procedures, which address the 10CFR73.21 and 10CFR2.390 program.
E1.2	Media Access				N/A
E1.3	Media Labeling/Marking				N/A
E1.4	Media Storage				N/A
E1.5	Media Transport				N/A
E1.6	Media Sanitation and Disposal	X	X	X	For licensees that utilize kiosks or scanning station for sanitization: For SGI and SRI information, the licensee's information protection is addressed by site procedures, which address the 10CFR73.21 and 10CFR2.390 program.
Appendix E2 Personal Security					
E2.1	Personnel Security Policy and Procedures				N/A
E.2.2	Personnel Termination/Transfer	X	X	X	The licensee/site ensures that admin access to kiosks is revoked or modified for individuals who no longer require access to the kiosks.
Appendix E3 System and Information Integrity					
E3.1	System and Information Integrity Policy and Procedures	X	X	X	Kiosks and scanning stations should be included as part of the site program to implement Appendix E3 requirements.
E3.2	Flaw Remediation	X	X	X	Kiosks and scanning stations should be included as part of the site program to implement Appendix E3 requirements.

Control	Control Title	Stand-alone	Networked	Program	Guidance
E3.3	Malicious Code Protection	X	X		An appropriate malware detection method for the kiosks and management consoles would include application whitelisting, periodic AV scans of the kiosk/management console hard drive and memory, and physical protection. Unless logs are being automatically forwarded to the plant-wide SIEM, review kiosk and management console logs every 14 days. For LAN-connected kiosks with a permanent management console the management console can be configured as a Syslog server and receive, consolidate and store logs from all of the kiosks which will eliminate the need to individually collect and review logs from each of the kiosks.
E3.4	Monitoring Tools and Techniques	X	X		Controls outlined in this document, specifically in E3.3 of this table ensure adequate protection of kiosks. Additionally, the following controls are implemented to ensure protection of the kiosk: • Kiosks are functionally tested (e.g., a test that verifies that signatures are functioning, such as the use of a benign virus signature file) every 14 days, and before being placed back in service after each repair or inoperative state. • Kiosks shall ensure that the encrypted files are not transferred or that appropriate provisions are being made if encrypted traffic needs to be transferred.
E3.5	Security Alerts and Advisories	X	X	X	The kiosks, management consoles and associated infrastructure should be included in the site's threat and vulnerability management program. Applicable vulnerabilities should be remediated in accordance with vulnerability management and work management processes and the guidance of Addendum 5 to NEI 08-09, Revision 6.
E3.6	Security Functionality Verification	X	X		System administrators should verify proper system functionality after maintenance or updating of a kiosk or maintenance console and prior to returning the kiosk stations back into service. Controls outlined in this document, specifically in E3.3 and E3.4 of this table ensure adequate protection of kiosks.
E3.7	Software and Information Integrity	X	X		Controls outlined in this document, specifically in E3.3 and E3.4 of this table ensure adequate protection of kiosks.
E3.8	Information Input Restriction				N/A
E3.9	Error Handling	X	X		Error conditions on kiosks are identified and Users are trained to not use the kiosk and notify the Administrators if error conditions are identified.
E3.10	Information Output Handling and Restrictions				N/A
E3.11	Anticipated Failure Response				N/A
Appendix E4 Maintenance					
E4.1	System Maintenance Policy and Procedures	X	X	X	Completion and approval of a kiosk control guidance document in accordance with this document will serve as the physical internal and administrative access control policy for kiosks and for management consoles.
E4.2	Maintenance Tools	X	X		Approve, monitor and document the use of digital maintenance tools used to maintain kiosks and, where applicable, management consoles. Control maintenance tools associated with kiosks and management consoles to prevent improper modifications. Maintenance tools include, for example, diagnostic and test equipment and mobile devices such as laptops. Checking and documenting media and mobile devices, such as laptops, containing diagnostic, system and test programs/software for malicious code before the media or mobile device is used in/on a kiosk or management console.

Control	Control Title	Stand-alone	Networked	Program	Guidance
E4.3	Personnel Performing Maintenance and Testing Activities	X	X		Maintaining and documenting a current list of authorized maintenance personnel consistent with its access authorization program and insider mitigation program, and Designating and documenting personnel with required access authorization and knowledge necessary to supervise escorted personnel interacting with kiosks and management console.
Appendix E5 Physical and Operational Environment Protection for Kiosks Located outside the PA					
E5.1	Physical and Operational Environment Protection Policies and Procedures	X	X	X	Kiosks located outside the PA should comply with the licensee's physical protection policy and the below E5 guidance.
E5.2	Third Party/Escorted Access	X	X	X	Network kiosks located outside the PA need to comply with the licensee's procedure controlling and documenting physical access to the kiosk device.
E5.3	Physical & Environmental Protection	X	X		Kiosks and management consoles should be located in a room with physical access control restrictions or in a locked cabinet in the case of management consoles. Physical controls, such as door locks or padlocks with keys controlled within an 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.
E5.4	Physical Access Authorizations	X	X		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 kiosks and management consoles. Designating officials within the organization to review and approve the above access lists and authorization credentials, consistent with the access authorization program.
E5.5	Physical Access Control	X	X		Kiosks and management consoles located outside of the PA should be protected by ensuring that they are located in areas/facilities with robust walls, ceilings, and doors to prevent unauthorized access or entry.
E5.6	Access Control for Transmission Medium		X	X	Network kiosks located outside the PA need to comply with the licensee's procedure controlling and documenting physical access to the Kiosk communication paths.
E5.7	Access Control for Display Medium	X	X		Access controls for kiosks located outside of the PA are met by implementing the controls defined in E5.1 through E5.5 of this table.
E5.8	Monitoring Physical Access	X	X		Locks, access control entry devices (i.e., key cards), or other means to ensure isolation and protection of kiosks and management consoles should be implemented in a way that ensures positive control and appropriately facilitates assessment of unauthorized access.
E5.9	Visitor Control Access Records	X	X		Kiosks located outside the PA should comply with the licensee's program to control and document physical access to kiosks and escorting visitors to prevent adverse impact to the kiosk function.
Appendix E6 Defense-in-Depth					
E6	Defense-In-Depth	X	X		Defense in depth involves placing multiple barriers between an adversary and the asset being protected. In the case of the kiosks, management consoles and network infrastructure, the barriers include physical protections, access controls, technical controls (e.g., application whitelisting, NIDS and passwords) and monitoring of logs. A summary of the defense-in-depth protection of the kiosks should be documented within the evaluation to demonstrate the measures taken to provide defense-in-depth protection of the kiosks. If on an isolated-LAN, then implement one-way data flows if sending logs or other information outside the LAN (e.g., log collector) using a deterministic device. If on an isolated-LAN with kiosks servicing different defensive levels, use hardware mechanisms (such as a firewall), to ensure that data always flows from the higher defensive to the lower defensive level.
Appendix E7 Incident Response					

Control	Control Title	Stand-alone	Networked	Program	Guidance
E7	Incident Response	X	X	X	Include attacks on the kiosk or management console applications as equipment that is considered in Cyber Incident Response drills/exercises and training.
Appendix E8 Cyber Security Contingency Plan (Continuity of Operations)					
E8	Contingency Plan				N/A
Appendix E9 Training					
E9	Training	X	X		Training for cyber security and plant personal should be provided to ensure adequate knowledge for those individuals administrating the kiosks and those personnel interfacing with kiosks to scan portable media and transfer data. Incorporate kiosk and management console functions and protection controls into the site training program.
E9.4	Specialized Training	X	X		Ensure training for staff configuring, updating (software and signatures) and maintaining kiosks and management consoles.
Appendix E10 Configuration Management					
E10.1	Configuration Management	X	X		A baseline configuration of kiosks and management consoles should be maintained and updated upon modification to kiosks and management consoles. Periodic signature updates and routine patching do not constitute a configuration change. However, software updates are considered to be a configuration change.
E10.3	Baseline Configurations	X	X	X	Baseline configurations of kiosks are maintained in accordance with E10.1 of this table. Controls outlined in this document ensure adequate protection of kiosks, specifically application whitelisting; kiosks/scanning stations hardening in accordance with D5 controls; physical protection (either within the PA or E-5 controls are applied) and 14 day log reviews. As a result periodic auditing of baseline configurations are not required to be performed on kiosks.
E10.8	Least Functionality	X	X	X	Baseline configurations of kiosks are maintained in accordance with E10.1 of this Table. Controls outlined in this document ensure adequate protection of kiosks, specifically application whitelisting, kiosks/scanning stations hardening in accordance with D5 controls; physical protection (either within the PA or E-5 controls are applied) and 14 day log reviews. As a result periodic auditing of unnecessary functions, ports, protocols, and services is not required to be performed on kiosks.
Appendix E11 System and Service Acquisition					
E11.1	System Services and Acquisition Policy	X	X	X	Develop policy and procedures to ensure kiosks and management consoles meet E11.6 requirements
E11.6	Licensee Testing	X	X		The objective of this control is to ensure that kiosks and management consoles are functionally tested and effective security controls implemented prior to introduction into a production environment or network, as well as throughout the system's lifecycle. Licensing testing should be performed in accordance with NEI 08-09, Revision 6 E11.6 and the guidance of Addendum 3 to NEI 08-09, Revision 6. Kiosks are considered "Commercial-Off-The-Shelf" (COTS)/ catalogue purchases thus vendor testing cannot be determined and adequate custody and control of the kiosk from the vendor to the licensee site until installation in the plant is not maintained. The requirements of E11.2 through 11.5 are through implementation of the guidance of Addendum 3 to NEI 08-09, Revision 6.
Appendix E12 Evaluate and Manage Cyber Risk					
E12	Evaluate And Manage Cyber Risk	X	X	X	Kiosks and management consoles should be included as part of the site program to implement Appendix E12 requirements and the guidance of Addendum 5 to NEI 08-09, Revision 6.