TRESYS TECHNOLOGY

XD AIR & NUCLEAR REGULATION

ADDRESSING NRC & NEI PORTABLE MEDIA GUIDANCE WITH XD AIR

INTRODUCTION

Nuclear Regulatory Committee (NRC) guidance states that secure data transfer must "ensure that the **data, software, firmware, or devices** are free from known malicious code, Trojan viruses, worms, and other passive attack." The scope of this regulation entails protecting against the full spectrum of portable media threats, including data-borne and device-borne threats. Traditional anti-virus (AV) scanning can address some of these threats, but not the full spectrum. Using Tresys XD Air™ in a secure deployment provides the full scope of protection against data, software, firmware, and device threats.

AV scanning protects against data and software threats by scanning for well-known Trojan viruses and worms. AV protection cannot address any other form of passive attack as required by the NRC regulation, and AV protection cannot provide firmware protection as required by the NRC regulation. While AV scanning can be used as part of a comprehensive solution to portable media protection, alone it is insufficient to meet the NRC regulations.

Tresys XD Air complies with NRC regulations and Nuclear Energy Institute (NEI) 08-09 guidance when properly integrated into facility processes and procedures for portable media security. Tresys provides a process and procedure template developed from successful inspections: http://www.tresys.com/products/datasheets/tresys_xdair_nuc_proc_template.pdf

NETWORK & DEVICE ISOLATION

NRC Regulatory Guide (RG) 5.71 (Section C.7) specifically requires a defense-in-depth architecture that "prevents remote access to CDAs [Critical Digital Assets] located in the highest defensive level".

The Security Defensive Architecture (SDA) defined in NEI 08-09 (Appendix A, Section 4.3) requires strict network isolation between higher security levels and lower security levels.

Isolation of high security areas leaves portable media as the only remaining attack vector from lower security levels. Portable media transfers are therefore a focus of great scrutiny during regulatory inspections.

NEI 08-09 (Appendix D Section 1.19), "Access Control for Portable and Mobile Devices" states that portable media devices (e.g., USB drives) cannot be moved between security levels. This requires maintaining a controlled inventory of portable media devices for each security level. Implementing this control in practice requires overlap with the Physical Access Control requirement from NRC RG 5.71, Section C.5.5.

DATA TRANSFER WITH XD AIR

While moving portable media devices across security levels is strictly prohibited, it is possible to move data across security levels by transferring it from one device to another. The NRC 5.71 regulatory guidance outlines the core requirements for performing secure data transfer, and the NEI 08-09 Appendix D Section 1.19 guidance

provides detailed controls for addressing the NRC guidance.

With XD Air it is possible to move data across security levels in a protected manner. XD Air is a boundary protection device for use in air gapped networks. A portable media device on one level can be used as input and a portable media device of another level can be used as output. With XD Air in a secure deployment it is possible to satisfy the NRC regulatory guidance and the detailed NEI controls.

Data Transfer with XD Air – NRC 5.71 Compliance

Per the NRC regulatory guidance, secure data transfer must account for **data, software, firmware, and device protection;** XD Air in a secure deployment addresses this full spectrum.

- **Data Protection:** XD Air performs deep content inspection of the data on the input device before transferring that data to the output device.
- **Software Protection:** XD Air performs multiple levels of AV checking before transferring any software to the output device.
- **Firmware Protection:** XD Air provides device isolation during the transfer to assure that no malicious firmware can be transferred between the input and output device.
- **Device Protection:** XD Air in a secure deployment allows for device-to-device transfer to be achieved while protecting the destination device.

With XD Air in a secure deployment it is possible to address the full spectrum of portable media threats defined in the NRC regulatory guidance. For more details about the data transfer capabilities of XD Air, see the datasheet here: http://www.tresys.com/products/datasheets/XD-Air-Datasheet.pdf

Data Transfer with XD Air – NEI 08-09 Compliance

From the NEI 08-09 Appendix D Section 1.19 controls, portable media protection:

- **"Authorizes, monitors, and controls device access to CDAs."**
  Addressing this control overlaps between technical implementation and physical security procedures. With physical security assurance that only a controlled inventory of devices can be used at each security level (see the Network & Device Isolation section above) it is possible to use XD Air to perform device authorization and monitoring for that controlled inventory.

- "Establishes and documents **usage restrictions** and **implementation guidance** for controlled portable and mobile devices."
  To adequately establish usage restrictions for portable media requires an overlap with practice & procedure as covered in the Practice & Procedure section. The recommended practice is to maintain a controlled inventory of secure media devices for use on high security networks.

- "Enforces and documents mobile **device security and integrity** are maintained at a level consistent with the CDA they support."
  To adequately enforce mobile device security and integrity are maintained while transferring data from one device to another, XD Air provides thorough data inspection and device isolation during the transfer. Data transfer with XD Air provides the full spectrum of protections required by the NRC guidance (see section: Data Transfer with XD Air – NRC 5.71 Compliance).

- "Enforces and documents mobile devices are used in one security level and **mobile devices are not moved between security levels**."
  Addressing this control requires implemented physical security procedures per the Physical Access Control requirement from NRC RG 5.71, Section C.5.5. See the "Network & Device Isolation" section above for more information.

With XD Air in a secure deployment it is possible to address the full spectrum of portable media threats defined in the NEI Appendix D controls. For more details about the data transfer capabilities of XD Air, see the datasheet here: http://www.tresys.com/products/datasheets/XD-Air-Datasheet.pdf

XD AIR CDA PROTECTION

As a boundary protection device XD Air is classified as a Critical Digital Asset (CDA) under the NRC guidance. NEI 08-09 Appendix B defines a CDA as a digital computer, communication system, or network that is:

> *"A component of a critical system (this* **includes assets that** *perform SSEP [Safety, Security, and Emergency Preparedness] functions;* **provide support to, protect, or provide a pathway to Critical Systems**)"

This is consistent with the regulation defense-in-depth architecture; a boundary device cannot provide protection against portable media threats to a broader network if the boundary device itself is not protected against those same threats. This protection must be sufficient to address the Design Basis Threat (DBT) defined by NRC which entails protecting against the full spectrum of data, software, firmware, and device threats.

NRC RG 5.71 Section C.7 requires that a device that performs data transfer across security levels be "trustworthy at or above the trust level of the device on which the data, code, information, or device will be installed or connected with." It is clear that a boundary protection device must meet the highest standards for security on cyber devices. Tresys XD Air was designed and developed specifically to provide this high level of trust. Full documentation about the secure XD Air architecture is available upon request.

NRC guidance explicitly includes firmware as a potential host for malicious code and an attack vector that must be addressed when transferring data across a security boundary. It is necessary to have a technical and procedural approach established that adequately protects against firmware based threats from portable media, such as BadUSB. For more information about how XD Air provides this firmware protection, see the Tresys BadUSB response: http://www.tresys.com/products/badusb.php

PROCESS & PROCEDURE IMPLEMENTATION

NRC Regulatory Guidance Section C.5.6, "Access Control for Transmission Medium", requires that the licensee, "controls and documents physical access to CDA communication paths." Given that the XD Air is itself a CDA, and as a boundary device presents a communication path to CDAs, this regulation requires implementing a physical process and procedure regarding usage of the XD Air.

For example, procedures implementing technical controls from NEI 08-09 Appendix D 1.19 include maintaining a set of known-good secure media devices for use in high security networks and assuring that only those devices are allowed to cross the "air gap" and connect to high security systems.

For more information about recommended practice & procedure using XD Air in the field, see our published document "Managing Mobile Media And The Secure Transport Of Ingress And Egress Data In Closed Environments": http://www.tresys.com/products/datasheets/tresys_xdair_nuc_proc_template.pdf

SUMMARY

Addressing portable media threats requires coordinating technical protections with secure process and physical security protections. Traditional AV scanning is not sufficient to address the full spectrum of technical threats from portable media. Any scanning done on a commodity system is insufficient to meet the CDA requirements for a boundary protection device. XD Air provides advanced content inspection built on a hardened platform to address portable media threats in a secure fashion not possible with traditional scanning systems.

XD Air provides the means to address technical controls per the NRC and NEI guidance. Using XD Air in a secure deployment along with the required physical security procedures allows sites to fully address portable media protection guidance. Because XD Air was developed to meet targeted threat requirements for secure government environments it is uniquely suited to protect against the DBT defined by the NRC.