

## **Addendum 3 to NEI 08-09, Revision 6 Dated April 2010 System and Services Acquisition**

### **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.11, “System and Services Acquisition.”

#### **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 System and Services Acquisition cyber security controls.

## **1.5 DEFINITIONS**

**Commercial Off-The-Shelf (COTS) Software** – Commercial devices or software (that is shipped and received with normal and expected vendor shipping packaging such as shrink-wrap, tamper seal or other recognizable packaging and marking) that is available from multiple sources developed to run as intended by the original developer. This would include such products as commercially available operating systems (i.e. MS Windows, Linux, OSX, TXS, etc.) general purpose application software, (i.e. MS Office, Corel, Open Office, SQL Server, etc.) and open source products whose builds can be verified and are obtained from known trusted sources. Firmware such as that for a BIOS, field upgradable commercial sensor (i.e. Pressure Transmitters, Flow Sensors, Level Sensors, etc.), or other off the shelf upgradable hardware (i.e. Hard Drives, Video Cards, DVD Drives, Embedded OS, etc.) would be considered COTS.

**Custom Software** – Any non-general purpose software product that has been customized to run on a hardware platform developed using any combination of commercial software and original coding to create an application or operating system that is purpose driven. This includes custom firmware designed to program or map hardware for a specific purpose (PLC, FPGA, EPROM and other programmable logic devices) and code that has been independently developed to enhance COTS software (portable code, macros, scripting, Visual Basic for Scripting, etc.)

## **2 SYSTEM AND SERVICES ACQUISITION GUIDANCE**

This section provides guidance related to the System and Services Acquisition cyber security controls in Appendix E, Section E.11 of NEI 08-09, Revision 6.

### **2.1 GENERAL GUIDANCE**

#### **2.1.1 Applicability**

The NEI 08-09, Revision 6, E.11, “Systems and Services Acquisition,” family of cyber security controls apply to the acquisition of CDAs, components of CDAs and services related to CDAs and components of CDAs following a licensee’s Cyber Security Plan full implementation date. CDAs that have been installed in the plant prior to the Cyber Security Plan full implementation date have already been through the acquisition and the associated licensee installation testing process, thus further action is not necessary to meet the E.11 requirements. However, the handling of these CDA must be addressed in the Systems Services and Acquisition policy and procedures and addressed in current CDA assessments. The E.11.6 requirement for audits of CDAs are applicable to previously installed CDAs as part of the ongoing monitoring and assessment process. The E.11 controls are applicable for the ongoing acquisition of parts or services associated with all CDAs.

#### **2.1.2 Maintaining Custody and Control of Devices or Software from a Vendor to Installation**

In order to use vendor-testing programs to meet the requirement of NEI 08-09, Appendix E, Section 11.5 requirements as a means to detect malware, the licensee must demonstrate that custody and control of the devices have been maintained from the vendor through the time period that the CDA/CS or software has been installed in the plant.

Licensee receipt processes shall ensure that devices or software were procured and expected to arrive and were received with normal vendor shipping packaging, such as shrink-wrap, tamper seal or other recognizable packaging and marking in place.

Control of the CDA/CS or software package shall be maintained and placed into segregated areas with access controls in place, that at a minimum meet the requirements, if located outside of the PA, of NEI 08-09, Appendix E, Section 5.5, “Physical Access Control,” to ensure that only authorized individuals have physical access to the materials while being stored prior to installation. For software, integrity of the software shall be maintained by verifying integrity of the software before use.

### **2.2 CYBER SECURITY CONTROL SPECIFIC GUIDANCE**

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

## 2.2.1 Appendix E.11.1, System and Services Acquisition Policy and Procedures

### Control language from NEI 08-09

This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, system and services acquisition policy that addresses the following:
  - The purpose of the security program as it relates to protecting the organization's personnel and assets;
  - The scope of the security program as it applies to the organizational staff and third-party contractors;
  - The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments.
- A formal, documented procedure to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

### Guidance

The objective of System and Services Acquisition Policy and Procedures is to ensure that licensees develop a formal, documented, system and services acquisition policy that addresses cyber security concerns and requirements in their purchase of CDAs and associated services and that licensees develop and deploy policies and procedures that address this objective. Licensees must develop and implement a formal, documented procedure to facilitate the implementation policy and associated system and services acquisition controls.

Applicability of Section E.11 Controls:

- **Safety-Related Direct CDAs** – Licensee Appendix B quality requirements meet many of the requirements of NEI 08-09, Appendix E, Section 11 requirements. Licensees need to ensure that cyber security requirements are included in the Safety-Related design and procurement process and that the gaps between the NEI 08-09, Appendix E, Section 11 requirements and the safety-related processes are evaluated and closed.
- **Non-Safety Direct CDAs** – The licensee non-safety-related procurement requirements must ensure that cyber security requirements are included in plant procurement programs.
- **Indirect CDAs** – Appendix E, Section 11 controls for Indirect CDAs can be addressed programmatically using normal site procurement standards such as :
  - Approved vendor list,
  - Receipt inspection,
  - Storage of CDAs,
  - Pre-installation testing.

## 2.2.2 Appendix E.11.2, Supply Chain Protection

### Control language from NEI 08-09

This security control protects against supply chain threats by employing the following measures to protect against supply chain threats and to maintain the integrity of the CDAs that are acquired:

- Establishment of trusted distribution paths,
- Validation of vendors, and
- Requirement of tamper proof products or tamper evident seals on acquired products.

### Guidance

The objective of this control is to ensure that items (including software) obtained from the supply chain are procured from trusted sources and those critical items have traceability and validation, such as a certification of compliance. The purpose of this control is to ensure that licensees take appropriate measures to protect their supply chain including vendor validation, tamper-proof packaging, and that CDAs meet defined levels of trustworthiness, and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

- Establishment of trusted distribution paths and validation of vendors;
  - Licensees must take reasonable measures to ensure that the vendor is a valid trustworthy business and that the shipping process is secure.
    - Safety-related equipment design and procurement standards may have measures in place to meet these requirements. However, these programs must be validated to meet these requirements or be modified if deficient in order to take credit for these programs.
    - For other Direct CDA procurement, a process must be developed to validate the vendors:
      - Validated vendor- Vendors must be evaluated and approved before conducting business. The vendor validation process includes attributes such as:
        - Ensuring a dealer or reseller is authorized by the vendor.
        - Verification of tax information as outlined in the Taxpayer Identification Number Form (W-9).
        - Verification of D-U-N-S number and information.
        - Assessment of influence of Foreign ownership.
        - In addition, vendors may be subject to public domain searches, assessment by a third party service and direct telephone contact from Procurement Services.

- The supplier's process defines the actions taken (e.g. access controls, scanning, testing, etc.) to ensure the integrity of systems and components (including the hardware and software components that compose those systems).
  - The licensee must understand the distribution paths and ensure that they comply with program standards.
  - For Commercial of the Shelf (COTS)/Catalogue and third-party purchases, the license must ensure that products come from a “validated vendor” which includes shipping from known, designated shipping points and is tested in accordance with section E.11.6.
- Requirements for maintaining custody and control of devices or software, and the use of tamper proof products or tamper proof seals.
    - In order to meet the requirements of NEI 08-09, Appendix E, Section 11.2 requirements, the licensee must demonstrate that the device or software is coming from a known source and that custody and control have been maintained from the vendor through the time period that the CDA/CS or software has been installed in the plant.
    - Licensee receipt inspection processes shall ensure that devices or software are shipped and received with manifest and expected vendor shipping packaging is in place, such as shrink-wrap, tamper seal or other recognizable packaging and marking.
    - Control of the package(s) shall be maintained and placed into segregated areas or are tampered sealed in order to identify attempts at unauthorized access, in locations with access controls in, that at a minimum meet the requirements, if located outside of the PA, of NEI 08-09, Appendix E, Section 5.5 to ensure that only authorized individuals have physical access to the materials while being stored prior to installation.
    - Software should be shipped in tamper evident packaging or protected by encryption, digital signatures and hashing algorithm is used to validate the integrity of software provided by the vendor Software on CDs, DVDs, Flash mass storage or other media that is not protected by tamper-evident packaging should be sent and stored in an encrypted format. Media passwords or access controls should be sent separately from the device.
  - In the absence of the above processes, the licensee takes on the responsibility to ensure that the testing in accordance with E.11.6 conducted prior to installation is robust enough to ensure that any known malware and vulnerabilities can be detected and addressed.

### **2.2.3 Appendix E.11.3, Trustworthiness**

#### **Control language from NEI 08-09**

This security control requires that CDAs meet defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

## **Guidance**

The objective of the Trustworthiness control is to ensure that acquired or developed software is free from known cyber security vulnerabilities as well as unauthorized and undocumented functionality and features. This security control requires that CDAs meet defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

The referenced requirements document should include applicable Software Quality Assurance (SQA) and cyber security program requirements that detail required actions to manage software quality and minimize the potential for flawed or malformed software.

Safety-related equipment design and procurement standards may have measures in place to meet these requirements but must be verified to ensure they meet these requirements.

For other Direct CS/CDAs and software, detailed purchasing specifications must be developed which includes configuration documentation, configuration validation, factory acceptance testing, and a cyber security program that minimizes flaws.

For catalog purchases, validated vendors under contractual obligations to reduce vulnerabilities must be used. In the absence of these controls, appropriate performance testing in accordance Section E.11.6 must be completed prior to installation.

## **2.2.4 Appendix E.11.4, Integration of Security Capabilities**

### **Control language from NEI 08-09**

This security control documents and implements a program to ensure that new acquisitions incorporate security controls based on the following:

- Being cognizant of evolving cyber security threats and vulnerabilities;
- Being cognizant of advancements in cyber security protective strategies and security controls; and
- Conducting analyses of the effects advancements could have on the security, safety and operation of the nuclear critical assets, systems, CDAs and networks at their facility.

## **Guidance**

The objective of this control is to ensure that the licensee's cyber security program remains effective over time as the threats, attack methodologies, and corresponding protective and detective measures evolve. The purpose of this control is to ensure that licensees establish guidelines for the integration of security capabilities into organizational acquisitions.

To ensure licensees integrate current security capabilities into new acquisitions:

- Ensure the procurement of CDAs is informed by the vulnerability and threat management program.
- Ongoing Monitoring and Assessment Effectiveness Analysis in accordance with Section 4.4.3.2 of the Licensee CSP considers advancements in protective strategies and security controls that improve performance of the Cyber Security Program and ensures that design and purchasing processes are maintained.
- Design cycle and purchasing process must be maintained to ensure linkage to the defensive strategy and Security Control Implementation Strategy.
- The Supplier or Licensee should document a cyber security impact analysis or other analysis that considers how assets could be exploited and the potential impacts of security control failures on CDA security and safety functions.
- New acquisitions incorporate program effectiveness and address potential vulnerabilities as it evolves in response to changing threats.
- The Licensee should work with the Supplier and have a process that ensures CDAs are developed and delivered in a way that addresses known vulnerabilities and considers potential failure modes. The engineering change process, typically will ensure that these failure modes would be evaluated for impacts on functionality.
- For COTS/catalogue purchases, if there is no or limited support by vendor programs or processes, the licensee is responsible for the role of the integrator and needs to address evolving cyber security threats and vulnerabilities and CDA failure modes and effects on SSEP functions and appropriate testing in accordance with Section E.11.6 prior to installation.

## **2.2.5 Appendix E.11.5, Developer Security Testing**

### **Control language from NEI 08-09**

This security control requires system developers/integrators of acquired CDAs create a security test and evaluation plan, implement the plan, and document the results such that:

- The products are delivered to meet specified security requirements, and
- The delivered product is free from known testable vulnerabilities and known malicious code.

This security control also requires the plan and results be reviewed and approved by the licensee.

### **Guidance**

The objective of developer security testing is to ensure that purchased software, or software delivered as a component of a CDA, is free of malicious, hidden, and/or unauthorized content or functionality and known vulnerabilities.

When the licensee utilizes a third party vendor to develop and acquire a CS/CDA, licensees should specify requirements for factory acceptance functional testing as part of the purchasing contract and ensure that the contract is augmented to include testing of the cyber security control implementations. As part of the control, licensees must review and approve security testing.

A Cyber Security procurement specification addresses:

1. Requirements for a CDA security evaluation and testing plans to demonstrate proper security control capabilities and functionality.
2. A Licensee requirement to review and approve CDA security evaluation and testing plans.
3. CDA security evaluation and testing plans that includes actions that provide reasonable assurance the delivered product is free from known testable vulnerabilities and known malicious code.
4. A Supplier process that includes steps that maintains the integrity of developed CDA software until the product is delivered.

For devices where there is no or limited knowledge of vendor programs or processes, such as for COTS/catalogue purchases, appropriate CDA Performance Testing must be performed prior to installation.

## **2.2.6 Appendix E.11.6, Licensee Testing**

### **Control language from NEI 08-09**

This security control:

- Requires testing (e.g., off-line on a comparable CDA) of security devices and software to ensure that they do not compromise the CDA or interconnected CDAs operation prior to installation, and
- Deploys security controls and flaw remediation measures based on reliable and credible sources of risk information.

This security control requires audits of CDAs, to provide high level of assurance that the safety, security, and emergency preparedness function are protected from a cyber-attack to validate the following items:

- Security controls present during system validation testing are still installed and operating in the production system,
- CDAs are free from known security compromises and continue to provide information on the nature and extent of compromises should they occur, and
- Management of change program is being followed with an audit trail of reviews and approvals for changes.

### **Guidance**

The objective of this control is to ensure that CDAs are tested for vulnerabilities and effective security controls prior to introduction into a production environment or network, as well as throughout the system's lifecycle.

Licensees programs should ensure that site acceptance testing is specified in the design cycle and procurement contract, and that site acceptance testing includes validation of the cyber security

control implementation. Configuration management activities must provide an audit trail of subsequent changes.

The programs include:

1. Site acceptance testing that validates proper security control capabilities and functionality prior to placing the CDA into production.
2. A documented vulnerability assessment or scan that concludes the installed CDA configuration is free from known vulnerabilities and known malicious code.
3. Requirements that changes made during installation and final testing are controlled in accordance with licensee configuration change control processes.

For devices where developer or vendor programs cannot be verified, such as for COTS/catalogue purchases and untrusted sources the licensee must ensure that appropriate controls are in place and testing as described below is conducted to ensure that CDA/CS and software have no vulnerabilities or malware prior to installation.

For complex or purpose built CDAs/CSs or software, testing should include:

- Testing of a CS/CDA in an isolated test environment, where the CS/CDA is then functionally tested to meet a documented software requirements test plan and the software quality assurance plan.
- Third party software products, which have been integrated into a software derivable product, shall be disclosed and known vulnerabilities identified. Software testing shall include input parametric testing of both valid and invalid input conditions to verify those conditions will not adversely affect the system/device. Software shall be tested against known testable vulnerabilities that would allow an attack to compromise the systems/device.

For “Commercial-Off-The-Shelf” (COTS)/ catalogue purchases where: the above testing cannot be accomplished; vendor testing cannot be determined; or, adequate custody and control of the Digital Asset from the vendor to the licensee site until installation in the plant is not maintained:

- If possible, determine what software development and QA is performed by the vendor, in order to take credit for the signature and performance testing that will reveal anomalous behavior;
- If unable to determine the testing performed by the vendor, perform functional, signature based and anomaly based testing to ensure that no malware exists on the device. This includes:
  - For low functioning, non-field modifiable devices (e.g., NEI 13-10, Appendix D, A.1, A.2 devices):
    - Signature based scans, if feasible; and,
    - Functional testing.

- For more complex devices (e.g., NEI 13-10, A.3 and higher):
  - Flash or wipe the device and re-image with controlled software and conduct functional testing;
  - Conduct vulnerability and malware scans of the device.
  
- For complex devices that cannot be flashed or wiped clean:
  - Vulnerability and malware scan of the device; and,
  - Conduct expanded functional testing including input testing of both valid and invalid input conditions to discover anomalies and verify those conditions will not adversely affect the system/device.