Addendum 2 to NEI 08-09, Revision 6 Dated April 2010 Cyber Attack Detection, Response and Elimination

1 INTRODUCTION

1.1 BACKGROUND

Title 10, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of the Code of Federal Regulations requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR Part 73, Section 73.1.

10 CFR 73.54 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan. Additionally, 10 CFR 73.54(e) requires that the cyber security plan must describe how the licensee will:

i. Maintain the capability for timely detection and response to cyber attacks;
ii. Mitigate the consequences of cyber attacks;
iii. Correct exploited vulnerabilities; and
iv. Restore affected systems, networks, and/or equipment affected by cyber attacks.

Further, 10 CFR 73.54(c)(4) requires the cyber security program be designed to ensure that the functions of protected assets are not adversely impacted due to 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, Section 2.2, discusses that the performance based requirements demonstrated in the Cyber Security Plan (CSP) that are designed to: (Section 2.2.13) Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1 at all times.

The guidance in this Addendum is applicable to any CDA. Where licensees may have used the guidance in NEI 13-10, "Cyber Security Control Assessments," the assessment elements in this Addendum would apply to Direct CDAs. Indirect CDAs have been previously assessed, in accordance with NEI 13-10, to justify the ability to detect and mitigate compromise prior to adverse impact.

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 the acceptable approaches to implement detection, response, and recovery elements of the Rule and CSP are 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 approaches to implement the cyber attack detection, response, and recovery elements of the Rule and CSP. This addendum intends to enhance clarity and consistency in implementation, and to support NRC oversight activities.

1.3 SCOPE

The guidance in this addendum is applicable to power reactor licensees with Cyber Security Plans (CSP) based on the template in NEI 08-09, Revision 6. The guidance in this Addendum is applicable to any CDA. Where licensees may have used the guidance in NEI 13-10, "Cyber Security Control Assessments," the assessment elements of this Addendum would apply to Direct CDAs. Indirect CDAs have been previously assessed, in accordance with NEI 13-10, to justify the ability to detect and mitigate compromise prior to adverse impact.

Section 2 provides a method to assess detection, response and elimination (i.e., mitigation or prevention) capabilities. Section 3 discusses the use of programs and processes for detection. Section 4 discusses the use of security operations centers, intrusion detection, and security information and event monitoring systems. Section 5 provides a series of examples consistent with the guidance in this document. The examples are intended to illustrate the level of detail appropriate for conducting an assessment of detection, response and elimination capabilities.

1.4 USE OF THIS DOCUMENT

This document may be used to implement the cyber attack detection, response, and recovery elements of the Rule and CSP for Direct CDAs. Where NEI 13-10 was used, Indirect CDAs would have been analyzed separately to determinate that any mal-operation can be detected and mitigated prior to adverse impact to SSEP functions

This document discusses the capability to detect, respond-to, and eliminate cyber attacks. In this context, the term 'eliminate' is inclusive of concepts of mitigation and prevention of the adverse impacts of a cyber attack.

1.5 ACRONYMS

The following acronyms are used in this document:

BIOS – Basic Input/Output System
CAP – Corrective Action Program
CD/DVD – Compact Disk/Digital Video Disk
CDA – Critical Digital Asset
CPU – Central Processing Unit
CSP – Cyber Security Plan

DCS – Distributed Control System
DRE – Cyber attack detection, response and elimination
HIDS – Host Intrusion Detection System
HMI – Human Machine Interface
I&C – Instrumentation & Control
I/O – Input/Output
IAW – In Accordance With
IDS – Intrusion Detection System
LAN – Local Area Network
MTE – Maintenance & Test Equipment
NIDS – Network Intrusion Detection System
OCA – Owner Controlled Area
PA – Protected Area
PC – Personal Computer
PLC – Programmable Logic Controller
PMD – Portable Mobile Device
QA – Quality Assurance
ROM – Read Only Memory
SIEM – Security Information and Event Management
SOC – Security Operations Center
SSEP – Safety-related and important-to safety functions, Security functions, and Emergency Preparedness functions including offsite communications
TCP/IP – Transmission Control Protocol/Internet Protocol
USB – Universal Serial Bus
VA – Vital Area

1.6 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 unmodified as delivered 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 DETERMINATION OF DETECTION, RESPONSE AND ELIMINATION CAPABILITIES

2.1 TIMELY ATTACK DETECTION

Timely detection can be demonstrated through the use of near real time automated capabilities, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway. One example of detection along an attack pathway is supply chain testing which includes anti-virus scanning and verification of proper equipment operation (i.e., detection for anomalous behavior).

When considering the timeliness of detection capabilities, a basis may be developed which is consistent with other evaluated and approved outage or compensatory time (e.g., technical specifications, physical security plan). When considering if a licensee has timely detection, the following questions should be asked:

1) Did the licensee place its detection capability along the attack pathway(s) at a location where it can detect cyber attacks and permit the licensee to respond and eliminate the cyber attacks before an adverse impact to the SSEP function?
2) Are personnel responsible for cyber attack detection trained in accordance with licensee training standards, and are they sensitive to the indications of a cyber attack?

2.2 ADEQUATE DETECTION

Does the licensee have the ability to:

1) Timely detect and respond to malicious activity utilizing:
   a) Known features or signatures (signature based); or
   b) Known anomaly or indicators (anomaly based) detection (automated if technically possible and manual if not).
2) Determine the cause of the security event (i.e., that it is cyber security related); and,
3) Mitigate or eliminate the threat using documented processes and strategies?

Information to consider when determining adequate detection:

1) Adequacy of detection:
   a) Are responders trained in accordance with licensee training standards on detection indicators?
   b) Does the licensee use whitelisting if technically possible?
2) Adequacy of signature based detection:
   a) If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators as required.
3) Adequacy of anomaly based detection:
   a) Does the licensee use anomaly detection indicators as part of its detection strategy and update the anomaly indicators as required.
4) Integrity of the Intrusion Detection System (IDS):
   a) If automatic IDS is used, is the IDS capable of detecting and preventing unauthorized changes to itself?

2.3 TIMELY ADEQUATE RESPONSE AND ELIMINATION

Response

Does the licensee have the ability to respond in a timely fashion to a cyber attack and eliminate the threat and prevent adverse impact to the SSEP function?

Information to consider when determining response ability:

1) Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on-site or on-call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber attack.
2) Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?

Information to consider when determining adequacy of personnel response:

1) Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?
2) Are procedures exercised and tested?
3) Is the equipment the personnel use for response available to them?
4) Is the environment the personnel respond adequate (environmental considerations addressed) to successful response?

Cyber Attack Elimination and Prevention of Adverse Impact to the SSEP Function

Does the licensee have the capability to use existing equipment or actions which prevents, eliminates or mitigates the adverse impact to SSEP function?

Information to consider when determining the adequacy of response and elimination of a cyber attack:

1) Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS/CDA?
2) Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?

3 DETECTION USING POGRAMS AND PROCESSES

Timely detection can be demonstrated through the use of near real time automated capabilities, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway.

Where technological methods for detection are not implemented, alternate methods (as described in Section 3.1.6 of the CSP) may be considered and implemented. When crediting alternate methods for detection, licensees should evaluate the methods and ensure they provide an adequate level of timely detection and timely response in order to prevent adverse impacts to the required functions (the goal is to ensure that the functions of protected assets identified by 10 CFR 73.54(b)(1) are not adversely impacted due to cyber attacks, not necessarily mal-operation of an individual CDA). The basis for crediting the alternate program should be incorporated into licensee documentation and sufficiently justified to withstand regulatory scrutiny.

Examples of programs and processes that may form the basis for alternate controls for detection include, but are not limited to:

- Operations rounds / operations monitoring
- Plant maintenance activities / troubleshooting procedures
- Plant modification testing / return to service testing
- System trouble alarms (annunciators) / plant computer alarms
- System engineering performance and condition monitoring software

For digital components not capable of advanced detection methods that were installed and operational prior to the full implementation of the CSP requirements, plant operating history and normal plant testing at the time of installation is sufficient to establish a baseline for anomaly detection for these devices.

3.1 USE OF SECURITY (IMP) OR OTHER ROUTINE ROUNDS FOR DETECTION

Where the licensee relies on Insider Mitigation Program (IMP) patrols or other routine rounds or surveillances to detect attempts to bypass access controls to a CS/CDA, the licensee ensures that the individuals are trained to recognize obvious indications of cyber tampering.

1) In the case of the CDA being located within the VA, the access monitoring and control mechanisms, site security program IMP rounds and 24/7 staffing of the control room provide an acceptable level of unauthorized physical access detection. Also, when CS\CDA maintenance is being performed, normal plant maintenance actions require verification by a technically knowledgeable individual to ensure proper completion of work orders and a closeout inspection of any collocated CDAs for evidence of tampering.
2) In the case of the CDA being located within the PA (but not the VA) then the licensee should consider additional controls for Direct CDAs or CDAs associated with the proper operation of Vital Equipment. In these cases, the use of physical tamper prevention and detection mechanisms (e.g. serialized tamper tape, port lock/blocking devices, locking enclosures, locking covers, or other positive means of detection, etc.), would provide an acceptable means for detecting unauthorized physical access and detection. Also, when

CS\CDA maintenance is being performed, normal maintenance actions require verification by a technically knowledgeable individual to ensure proper fulfilment of work orders and a closeout inspection of any collocated CDAs for evidence of tampering.

3.2 USE OF SYSTEM AND SERVICES ACQUISITION CONTROLS FOR DETECTION

The cyber security controls in NEI 08-09, Appendix E, Section 11, "System and Services Acquisition," can provide means for detecting cyber attacks. This section discusses the use of testing and custody and control elements for detection.

3.2.1 Detection through Testing Methods

Detection through testing is adequately accomplished by installing software on a comparable CS/CDA in an isolated test environment, where the CS/CDA is then functionally tested to identify anomalous behavior and meet a documented software requirements test plan and the software quality assurance plan.

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

1. 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.
2. 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:

1) 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;
2) 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:
   a) For low functioning, non-field modifiable devices (e.g., NEI 13-10, Appendix D, A.1,A.2 devices):
      i) Signature based scans, if feasible; and,
      ii) Functional Testing.
   b) For more complex devices (e.g., NEI 13-10, A.3 and higher):
      i) Flash or wipe the device and re-image with controlled software and conduct functional testing;
      ii) Conduct vulnerability and malware scans of the device.
   c) For complex devices that cannot be flashed or wiped clean:

i) Vulnerability and malware Scan of the device; and,
ii) 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.

3.2.2 Maintaining Custody and Control of Devices or Software from a Vendor to Installation

In order to use vendor-testing programs to meet the NEI 08-09, Appendix E, Section 11.5, "Developer Security Testing," control as a means to detect malware, the licensee should 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 should 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 should 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.

4 USE OF OPERATION CENTERS AND CENTRALIZED DETECTION

4.1 USE OF A SECURITY OPERATIONS CENTER (SOC)

Licensee may utilize a Security Operations Center (SOC) as a component of their detection, monitoring and response implementation. The use of the SOC should be documented and incorporated as a component of the licensee's procedures and processes. The information and logs sent to the SOC should be evaluated against existing licensee procedures for security sensitive information protection and records retention to ensure that appropriate requirements are implemented. Where necessary, based on the classification of the information, the licensee should provide technical methods to protect information in transit and at rest in accordance with licensee procedures.

Where SOC services utilized are provided by a third party (including a non-nuclear entity within a utility), a Service Level Agreement (SLA) or similar document should be established to outline the roles and responsibilities of all groups involved. The SLA should also outline the lines of demarcation between the licensee and the service provider.

It is not anticipated that personnel at a corporate or third party SOC have access, extensive knowledge, or administrative control over plant digital computer and communication systems that warrant inclusion in the "critical group" as described in 10 CFR 73.56.

4.2 DELAY IN IMPLEMENTATION OF INTRUSION DETECTION OR SECURITY INFORMATION AND EVENT MONITORING (SIEM) SYSTEMS

This section provides guidance for crediting alternate methods of cyber attack detection where a planned Intrusion Detection System (IDS) or Security Information and Event Management (SIEM) system installation cannot be completed prior to the full program implementation date. The guidance in this section should be considered in cases where the licensee cannot implement alternative controls for detection described in the other sections of this document.

In the case where the licensee has planned to implement an IDS on a **safety system** (and this activity is recorded in their CAP) but this has not been accomplished by the full implementation date due to the need for a scheduled outage, the licensee must show that required changes could not be accomplished without an outage. (Note: installing a NIDS may not require taking a system down/out-of-service to accomplish its installation but implementing a HIDS does.) The licensee shall implement the alternate security measures below to provide the ability to detect a cyber compromise before adverse impact to the SSEP function. The following actions would be considered adequate alternate security controls, provided the completion of the corrective action and IDS installation is completed within sixty days (to permit adequate close out of the change package) of the last day of the outage.

In the case where the licensee has planned to implement an IDS on a **security system** (and this activity is recorded in their CAP) but this has not been accomplished by the full implementation date, the licensee must show that required changes could not be accomplished without a delay beyond the full implementation date. (Note: installing a NIDS may not require taking a system down/out-of-service to accomplish its installation but implementing a HIDS does.) The licensee shall implement the alternate security measures below to provide the ability to detect a cyber

compromise before adverse impact to the SSEP function. The following actions would be considered adequate alternate security controls, provided the completion of the corrective action and IDS installation is completed within six months of the full implementation date.

Alternate measures for monitoring until installation of the planned IDS:

If the CS/CDA is located within the **Vital Area**:

1) The CS/CDA is monitored by IMP patrols and/or continually manned by personnel in the critical group;
2) The CS/CDA audit/logging functionality, if technically supported, is implemented and enabled and the logs extracted, reviewed and a report on the contents generated, at least once a month;
3) The CDAs performance is tested or verified against a secondary or alternate indicator weekly and when required to make operational decisions;
4) The CS/CDA is isolated with no communication pathways to other systems. If the CS/CDA communicates with other systems/devices then those systems/devices meet the same criteria as described above in 1 through 3;
5) The licensee's PMMD program has been inspected and found to be adequate; and,
6) The licensee installs a non-disclosed method of timely detection on the system.

If the CS/CDA is located within the **Protected Area** but outside the VA:

1) The CS/CDA audit/logging functionality, if technically supported, is implemented and enabled and the logs extracted, reviewed and a report on the contents generated, at least once a month;
2) The CS/CDA performance is tested or verified against a secondary or alternate indicator weekly and when required to make operational decisions;
3) Visible tamper indicators are used, surveyed and documented by plant personnel once every 24 hours and/or the CS/CDA is within a locked and alarmed enclosure or monitored by continuous video surveillance;
4) The CS/CDA is isolated with no communication pathways to other systems. If the CS\CDA communicates with other systems/devices then those systems/devices meet the same criteria as described above in 1 through 3;
5) The licensee's PMMD program has been inspected and found to be adequate; and,
6) The licensee installs a non-disclosed method of timely detection on the system.

If the CS/CDA is located **outside the PA**:

1) The CS/CDAs are located in areas that meet the requirements of NEI 08-09, Appendix E, Section 5;
2) The CS/CDA audit/logging functionality, if technically supported, is implemented and enabled and the logs extracted, reviewed and a report on the contents generated, at least once a month;
3) The CS/CDA performance is tested or verified against a secondary or alternate indicator weekly and when required to make operational decisions;
4) Communication pathways into the CS/CDA (including the communication media) are physically secured against tampering and surveyed weekly, and the other systems/devices

with which the CS/CDA communicates meet the same criteria as described above in 1 through 3;

5) The licensee's PMMD program has been inspected and found to be adequate; and,
6) The licensee installs a non-disclosed method of timely detection on the system.

5 DETECTION, RESPONSE AND ELIMINATION EXAMPLES

Below are examples of various components and systems, and acceptable ways to answer affirmatively the DRE filter questions provided in Section 2. In accordance with Section 3.1.6 of the CSP, alternate controls/countermeasures may be implemented that eliminate threat/attack vector(s) associated with one or more of the cyber security controls. These can be employed by performing an analysis and documenting the basis for implementing an alternative countermeasure which provides cyber security protection commensurate with the corresponding cyber security control.

The examples in this section below do not provide detailed information about system architecture nor processes, but does include alternate controls and standards that are acceptable for detection and response.

5.1 EXAMPLE 1: STANDARD COMPUTER SYSTEM

This computer system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The system has many connections and nodes,
- The system is running Microsoft Windows operating system, and
- The system supports fully functioning NIDS and HIDS.
- This computer system is isolated with no other connectivity.
- The attack pathways into this system are by way of USB drives, CD/DVD drives, wireless networks, and vendor MTE laptops.
- The licensee has an effective and adequate PMD protection program, which prevents known malware infected USB drives and CD/DVD from accessing the system.

Where along the attack pathway will the licensee detect a cyber attack?

Detection along the threat pathway includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable media__X__

IDS (HIDS/NIDS) __X_

Access Control____

Wireless_X__

Operator __X___

IMP__X__

The "X"ed items are potential areas that can used to detect a cyber intrusion along the threat pathway. The pathway includes supply chain, portable media devices, wireless networks, and HMIs.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	HIDS/NIDS has been installed and implemented in threat attack pathway to detect cyber attack.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are training IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	The system uses whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates signature indicators as required.
Adequacy of anomaly based detection		

Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	HIDS/NIDS is protected with anomaly detection capability.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	HIDS/NIDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses the Corporate SOC as the 24/7 basis as well as onsite monitoring and response.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee onsite CSIRT and SOC personnel are appropriately trained, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive and respond to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop drills and exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond to adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.

Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee training standards.

5.2 EXAMPLE 2: COMPUTER SYSTEM EXAMPLE A

System description

- Computer System is being upgraded as part of the full implementation cyber security program implementation and to address equipment obsolescence. The computer system is not safety-related but it provides an SSEP function.
- The Computer System includes a lot of connections to field devices. Outside of the field devices, which are part of the overall SSEP system, no other connections are provided to other systems so the Computer System is air gapped from any other plant systems, in Level 4 of the defensive architecture.
- Upgraded system is designed to be cyber security compliant with the cyber security plan. An intrusion detection system (IDS) function, intrusion prevention system (IPS) function and security information and event management (SIEM) function will be included in the upgraded system.
- Whitelisting will be built in to the upgraded system.
- No wireless capabilities are included in the Computer System.
- Equipment cabinet access controlled through the key control program and work management processes.
- Equipment cabinets contain alarm connections which result in alarm when opened.
- PMMD program used to ensure secure connections with removable media.
- Cyber testing performed during Factory Acceptance Testing and Site Acceptance Testing. Software controls included in the vendor activities for software requirement development, software design, software testing, and software V&V. Vendor has cyber security program and testing capabilities.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	SIEM, HIDS/NIDS, IPS has been installed and implemented in threat attack pathway to detect cyber attack. PMD control program will detect known malware on portable media and devices.

		System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured. The cabinets are in vital area and access control notifications alarmed and a location staffed 24/7.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	The system uses whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates signature indicators as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	HIDS/NIDS performs anomaly detection capability and updates indicators as required.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	HIDS/NIDS is configured to detect unauthorized changes to itself.

Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses the Corporate SOC as the 24/7 as well as onsite duty analyst or 24/7 response onsite and CSIRT for monitoring and response. If using corporate SOC, information is protected in accordance with site information protection standards such as VPN or encryption. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee onsite and SOC personnel are appropriately trained, in accordance with training standard.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standard.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		

Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures.

5.3 EXAMPLE 3: COMPUTER SYSTEM EXAMPLE B

System Description:

- System includes servers, workstations and firmware-based components.
- System has fully functional SIEM including custom developed SIEM rules.
- Logs are centrally collected by SIEM from devices that have the ability to send logs.
- SIEM provides notification of an identified abnormal condition in near real-time.
- System does not utilize NIDS.
- Whitelisting, HIDS, data loss prevention, and antivirus software are enabled, and sends logs to the SIEM.
- Wireless capability is disabled.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	SIEM, HIDS, IPS has been installed and implemented in threat attack pathway to detect cyber attack. PMD control program will detect known malware on portable media and devices. System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured. The cabinets are in vital area and access control notifications alarmed in a location staffed 24/7.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are training in accordance with licensee training strategies and procedures.
Adequate detection:		

Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	The system uses whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates signature indicators as defined in procedures.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	SIEM has the ability to performs anomaly detection and anomaly indicators are updated as they become available.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	HIDS is configured to detect unauthorized changes to itself .
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst for monitoring and CSIRT for response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm	Yes	Licensee onsite are appropriately trained, in accordance with training standards.

conditions?		
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond adequate to successfully response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures.

5.4 EXAMPLE 4: VINTAGE COMPUTER SYSTEM

Background

- Not feasible to replace the current vintage Computer System prior to Milestone 8 implementation date.
- Current plan is to use the current Computer System for a short time until completion of the upgrade in Q1-2018.
- New system will meet all Detection Response and Elimination control requirement

Current Vintage Computer System attributes

- Windows Server 2003
- Open VMS Servers
- Windows XP Workstations
- Standalone Level 4 system
- Nortel Network Switches – Server / Workstation / MUX communication
- MUX Boards – Field Device signal inputs and response / Conversion to network data / Generating Fault Alarms
- All equipment in the PA, except for some field I/O equipment
- Cables in hardened conduit with intrusion monitoring on junction boxes
- Field devices - Inaccessible interface ports, fault alarms to continuously manned locations.
- Continuously manned locations with strict access control.
- Locked cabinets for servers.
- Add Port Lockers for exposed ports, with periodic monitoring. (Switches in open cabinets)
- Port Blocking on exposed equipment with periodic monitoring
- Add virus protection to Servers / Workstations with manual updates and local management.
- Increase / validate OS security event logging on Servers and Workstations.
- Manual log collection with connector to SIEM for use case alerting

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	Anti-virus is installed in the threat attack pathway on the Windows workstations to detect cyber attack. Manual log collection with a connector to a SIEM for alerting and response before adverse impact. Monitored port blocking and PMD control program will detect malware on portable media and devices. System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured. Any hardware/software changes made to the system is tested to detect anomalous behavior. The cabinets are in vital area and access control notifications alarmed and a location staffed 24/7.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not used because patching of the systems is not allowed -there is no vendor support and this attack pathway does not exist. Any changes made to the system are tested to detect anomalous behavior. No software changes are

		allowed on the system. PMMD program in place for extraction of system data and logs performed bi-weekly.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates antivirus signature indicators as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Periodic functional tests of the equipment will indicate anomalous behavior. No software changes are allowed on the system.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	AV software is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses the Corporate SOC as the 24/7 as well as onsite duty analyst and CSIRT for monitoring and response. Manual Logs are sent to SOC for evaluation bi-weekly. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee onsite and SOC personnel are appropriately trained, in accordance with training standards.

Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises in accordance with licensee procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance with licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures.

5.5 EXAMPLE 5: DIGITAL DISTRIBUTED CONTROL SYSTEM EXAMPLE A

This control system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The digital distributed control system uses a multi-channel, "voting" scheme based on PLC technology that incorporates microprocessors to execute the monitoring and protection logic.
- These devices are "programmable"; definition of the logic functions are user configurable and alterable in the field with the use of the vendor's configuration software tools.
- Basic firmware that interprets and executes the user-defined logic burned in ROM and not field-alterable or upgradable.
- A PC workstation running Microsoft Windows operating system and fully functioning HIDS, is used for system configuration and a local high-speed communication interface is used to connect with the control system for configuration purposes.
- Interface is based on Ethernet-TCP/IP protocols.
- The configuration workstation is permanently connected to the SSEP system as opposed to temporarily being connected when configuration changes are required.
- USB ports
- Control system in Level 4 behind a one way deterministic boundary device with no bypasses.
- The licensee does not require the vendor to maintain an effective PMD program nor ensure integrity of the software and information flow which is introduced by vendor representatives

Detection along the Attack Pathway Includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable media__X__

IDS (HIDS/NIDS) _X__

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	Workstation HIDS. PMD control program will detect known malware on portable media and devices. System and Services Acquisition controls IAW with the CSP that ensure testing for anomalous behavior are in place that will detect malware in devices being procured.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is used.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The licensee updates antivirus signature indicators as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly detection is used and updated as required. Signature and anomaly Detection through System and Services Acquisition testing methods is conducted for new software

		introduction.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is capable of detecting unauthorized changes on itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		

Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedures have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.6 EXAMPLE 6: DIGITAL DISTRIBUTED CONTROL SYSTEM EXAMPLE B

Background

- Not all components are located in the Main Control Room (MCR); the cabinets are alarmed to an annunciator in the MCR.
- The system does not contain a Microsoft Windows PC connected for normal system operations.
- Components are dedicated and not swapped between SSEP and non-SSEP systems.
- USBs are not used with this system, but laptops are controlled in accordance with the PMD program.
- System undergoes rigorous calibration and functional checks during outages and limited portions are tested while online.
- This is a Level 4 networked system; hardware design prohibits incoming connections.
- Plant Operations personnel continuously monitor plant parameters associated with this system. Abnormal operation or indication would be identified by operations personnel.
- Access to the cabinets is alarmed to the main control room, unauthorized attempts to access the equipment would detected by indications in the MCR.
- This equipment is located in a locked and alarmed cabinet, which is monitored 24x7 by the MCR.
- Wireless functionality is not supported
- Rogue wireless scans are performed in areas around the computer systems.
- Surveillance instructions and calibrations are performed on this equipment.
- PMD control provides adequate protection to mitigate and detect the PMD attack vector.
- Procurement of devices in accordance with System and Services Acquisition cyber security controls in the CSP would detect
- This equipment is located in VA within locked and alarmed cabinets that have a key control program. Alarms are sent to annunciators in the MCR when cabinet doors are opened.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	The system does not contain a Microsoft Windows PC connected for normal system operations. Operations personnel continuously monitor plant parameters associated with this system. Abnormal operation or indication would be identified by operations personnel. Access to the cabinets is alarmed to the main control room; unauthorized attempts to access the equipment would be detected by indications in the MCR. USBs are not used with this system, but laptops are controlled in accordance with the PMD program and software from the vendor is screened. Detection through System and Services Acquisition testing methods is conducted for new software introduction. System undergoes rigorous calibration and functional checks during outages and limited portions are tested while online. Hardware design prohibits incoming connections Any changes made to the system are tested to detect anomalous behavior.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		

Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible for this system. Any changes to the processor configuration or to the software will be identified during rigorous calibration and functional checks during outages and limited portions are tested while online. Operations personnel continuously monitor plant parameters associated with this system. Abnormal operation or indication would be identified by operations personnel. The cabinets are located in the Vital Are or in the PA, access to the cabinets is alarmed, and unauthorized attempts to access the equipment would be detected by indications in the main control room.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection is not technically possible. See above for detection capabilities. Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly detection is not possible, but by abnormal operation or indication would be monitored and identified by operations personnel. Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	The systems does not have and IDS capability, but abnormal operation or indication would be monitored and

		identified by operations personnel.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst for monitoring and CSIRT for response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		

Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.7 EXAMPLE 7: DIGITAL REACTOR PROTECTION SYSTEM

Background

- Digital Reactor Protection System (RPS) was upgraded in 2009-2011 due to equipment obsolescence
- Four-channel system uses voting scheme to determine the need to trip the control rod drive breakers to protect the reactor at predetermined trip set points. The system is safety-related and provides an SSEP function.
- Self testing and diagnostic functions provided in the system design capabilities
- Digital RPS is located in Level 4 behind a data diode.
- Digital RPS connection to plant computer through a port tap aggregator one-way connection.
- No wireless capabilities are included in the Digital Reactor Protection System
- Does not include HIDS or NIDS capability in the current system design
- The system can be configured using the Monitoring and Service Interface, which is built into the system. Configuration controlled by the design change process and implemented with plant procedures.
- Monitoring and Service Interface through a Service Unit work station located in the control room. Bi-directional connection between the Service Unit and the safety processors. The Service Unit uses a Linux operating system. The Service Unit Service unit connection is a continuous connection. Interface between the Service Unit and the safety processors is controlled by the key switch module in each cabinet.
- Key switch module controls the operation mode of the system. Key switch must be placed in change-enabled mode in order for configuration changes to be made. Key switch key is control via the key control program and the key switch module is located in the cabinet. Key switch position parameter change enable position is provided to the control room via annunciator alarm.
- A maintenance laptop is available for the system and is stored in a cabinet in the Control Room. Laptop dedicated to the Digital RPS and only includes the software needed to interface with the digital system. The laptop uses a Linux operating system. The system run time environment software is written so the laptop can only be connected when a channel is out of service because the associated connector is not recognized by the safety processor during normal processing cycles.
- Equipment cabinet access controlled through the key control program and work management processes
- Equipment cabinets contain alarm connections which result in control room annunciator alarm when opened

- PMMD program used to ensure secure connections with removable media
- Cyber testing performed during Factory Acceptance Testing and Site Acceptance Testing. Software controls included in the vendor activities for software requirement development, software design, software testing, and software V&V. Vendor has cyber security program and testing capabilities.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Vendor representatives are not granted access to the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System does not support IDS, however, anomalous behavior would be detected because Monitoring and Service Interface has built in detection so that preconfigured messages, which are in the correct format and not faulted will be accepted. Faulted messages are ignored. Faulted signals are alarmed. The safety processors have self-testing and functional verifications, which are performed continuously, and any faults or deviations are alarmed. Configuration changes can only occur when the key switch module is placed in the parameter change enable mode by turning the key in the module. The key switch must be accessed by opening the cabinet, which is locked. The key for the key switch and for the cabinet are controlled by operations in the key control program. Prior to issuing the key switch key, the associated channel is placed in either bypass of trip condition. Cabinet access control notifications built into the system design such that physical access into the cabinets will be alarmed in the control room by annunciator. Key switch mode is alarmed when the key

		switch is placed in the parameter change enable mode. Channel check verification performed by operation personnel each shift. System and Services Acquisition controls IAW the CSP will test and detect any new software introduced for anomalous behavior into system
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, V&V and installation. No additional code or modification is authorized IAW with the NRC approved safety system licensing basis document.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection is not technically possible on the system. See above for detection capabilities. Detection through System and Services Acquisition testing methods is conducted for new software introduction. System design results in any effort to

		change the code will alarm and notify operators who will take appropriate action in accordance with approved procedures.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly detection is not possible on the system, but by system design any effort change the code will alarm and notify operators who will take appropriate action in accordance with approved procedures. Detection through System and Services Acquisition testing methods is conducted for new software introduction.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	Detection of unauthorized changes by an IDS system is not available, but by system design any effort change the code will alarm and notify operators who will take appropriate action in accordance with approved procedures.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in

licensee training standards, and sensitive to indications of a cyber attack?		accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.8 EXAMPLE 8: STANDARD LEGACY COMPUTER SYSTEM (PLANT COMPUTER)

This computer system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The legacy computer system is a central data acquisition and display system that collects real-time measurements from process areas all around the plant including the numerous isolated subsystems, using a combination of analog/contact/pulse input signals and point-to-point communication connections.
- It is based on a legacy computer and networking technology.
- This system also provides real-time plant information to the NRC and, in emergency situations, to off-site emergency monitoring and response facilities setup by the licensee.
- Systems also feed plant data to separate plant historian systems.
- The connectivity to diverse subsystems usually includes communications with meteorological stations geographically dispersed around the OCA and surrounding areas.
- Includes a gateway device in the computer room to make plant data available to other systems via TCP/IP networking but the gateway device is connected to a one-way boundary device.
- The computer system has numerous serial communication channels that go out to various smart devices and subsystems around the plant and local area. These serial communication circuits are individually managed by separate application programs that use them to “poll” and receive data value updates from those devices/subsystems.
- These application programs process the in-coming messages a character at a time and will immediately reject and flush any message that does not conform to the protocol specifications. They also do not accept ad-hoc messages from those devices/systems and any such message traffic would be rejected as spurious and unsolicited.
- The protocols used incorporate message length information (and maximum allowed message sizes) and so buffer-overflows are not a consideration.
- Operators double-check critical values against multiple sources.
- For the out-going data supplied by the computer system to external systems (e.g. plant historian, NRC, off-site monitoring) this data passes through a one-way boundary device that precludes incoming information flow.
- The system has physically distributed I/O multiplexors that are used to read analog, contact and pulse signals and convert them into measurement values, which can be trended, displayed and alarm checked by application software in the servers.
- The communications between the computer and the I/O multiplexors is a proprietary message protocol. The I/O LAN is a proprietary hardware design.

- This system supports an early version of Ethernet with a legacy network (which is not TCP/IP based.)
- System supports removable media in the form of cartridge tape modules and pre-dates the development of floppy disks and USB devices.
- Communication software on this system used to communicate with "smart" devices and subsystems, was custom-developed by the system integrator and not a commercially available application.
- The operator displays in the control room are generally "dumb" terminals or slaves to operator display applications running on the central computers.
- There are Personal Computer workstations emulating the virtual functionality connected to each of the redundant computers. The computers provide both real-time plant information, including reactor optimization calculations, as well as running specialized application programs that support emergency response activities. The programs on this system are no longer supported by a vendor.

Detection along the threat pathway includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable media__X__

IDS (HIDS/NIDS) ___

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	To address detection, the licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and

		elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices. Access control for HMI/Keyboard, critical values checked, software changes are verified against signature and anomaly based indicators.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	System does not support whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The system does not support Signature based detection. However, System and Services Acquisition controls IAW with the CSP are in place that will detect malware in devices being procured prior to introduction into the plant systems. PMD control program will detect malware on portable media and devices. Access control for HMI/keyboard, critical values checked, software changes are

		verified against signature and anomaly based indicators.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indication is not supported by this system. However, anomaly testing as part of the System and Services Acquisition controls are used. Also, operators monitor these systems 24/7 and will be able to detect anomalous behavior in plant equipment.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is not supported on installed equipment, but is supported in equipment used a part of supply chain and acquisition equipment used to ensure adequate testing prior to being installed in plant systems.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.

to indications of a cyber attack?		
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.9 EXAMPLE 9: LEGACY COMPUTER SYSTEM EXAMPLE A

Background

- Legacy Computer System is not safety-related but it provides an SSEP function.
- The Legacy Computer System includes a lot of connections to field devices.
- Connections to other plant systems such as control systems and monitoring systems are provided through the local area network, which is the infrastructure, built into the Legacy Computer System.
- An intrusion detection system (IDS) function and security information and event management (SIEM) function will be included in the local area network that the Legacy Computer System uses to connect to the other systems.
- Whitelisting is not included in the Legacy Computer System or the local area network infrastructure.
- No wireless capabilities are included in the Legacy Computer System
- Equipment cabinet access controlled through the key control program and work management processes
- PMMD program used to ensure secure connections with removable media
- Software controls included in the vendor activities for software requirement development, software design, and software testing.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System has IDS and a SIEM, which monitors connections within the plant LAN that is the interfacing system between the plant computer and the other plant digital control and monitoring systems. Any changes to the processor configuration or to the software will be performed by the design change process, which includes requirements for design development (hardware and software),

		testing, and installation. The licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices. Access control for HMI/Keyboard, will ensure control of this equipment.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible because the system is a legacy system and is not supported anymore and the system may become unstable with whitelisting installed.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within	Yes	Signature-based detection indicators are updated as required.

(frequency)?		
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indictors are accomplished as part of the App E section 11 System and Services Acquisition program. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, and installation Detection through System and Services Acquisition testing methods is conducted for new software introduction. The IDS noted on the LAN also performs anomaly detection. Operators also monitor plant other confirmatory plant equipment 24/7 and will identify anomalous equipment behavior.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.

conditions?		
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.10 EXAMPLE 10: LEGACY COMPUTER SYSTEM EXAMPLE B

Background

- Non-Windows OS with limited OEM support, and modern TCP/IP networking protocols in use.
- Configures on the CPU are such that network traffic is dropped unless ports and protocols are explicitly defined.
- Tapes are not used.
- Interfaces are licensee developed and supported.
- Satellite display terminals are Windows PCs with a GUI-based application.
- The equipment is located in the PA and VA within locked cabinets with key control, or protected with tamper seals, or located in a 24/7 manned area, or identification/authentication mechanisms (e.g.. usernames/passwords) are used.
- The SIEM deployed in accordance with procedure requirements provides mechanisms to identify and notify individuals of abnormal cyber conditions on the system.
- Notifications of events identified by the SIEM are sent to the cyber security analysts for investigation. The SIEM collects logs from systems, which support log forwarding including HIDS, Anti-Virus, Rogue System Detection, and Data Loss Prevention.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	Centrally managed antivirus, whitelisting, and data loss prevention software is deployed and monitored by SIEM to detect and prevent malicious software or unauthorized PMD use. The SIEM collects logs from systems, which support log forwarding including HIDS, Anti-Virus, Rogue System Detection, and Data Loss Prevention. PMD control provides adequate protection to mitigate and detect the PMD attack vector. Portions of this system are located in an area manned 24/7. Personnel stationed in the area would detect signs of malicious

		activity. Procurement and testing of devices in accordance with System and Services Acquisition cyber security controls would detect anomalous behavior.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Centrally managed whitelisting is deployed and monitored by SIEM to detect and prevent malicious software.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection indicators are updated as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	The licensee uses anomaly indicators as part of its detection strategy and updates the anomaly indicators as needed. Personnel trained to detect abnormal operation of the equipment. Training of personnel includes their role specific training and role based cyber security training.
Integrity of the Intrusion Detection System		

If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	Yes, the IDS has whitelisting installed, which would detect changes on itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee use a cyber security operations center manned and trained, in accordance with licensee training standards, personnel to assess and respond to cyber attack alarm conditions?	Yes	The licensee uses onsite or on call 24/7 duty analyst and CSIRT for monitoring and response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber	Yes	Procedure have been developed and

attack threat relative to the CS?		implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.11 EXAMPLE 11: MICROPROCESSOR BASED I&C SYSTEM EXAMPLE A

This I&C system is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- The digital I&C system is a multi-functional mainframe data acquisition and control system associated with an SSEP function.
- This system is a highly functional digital system with a CPU, firmware, memory, HMI, digital and analog I/O with serial and Ethernet communications capability and the system is located in the control room.
- The chassis is designed to be modular and therefore share common components with other systems, both those associated with SSEP functions and those not associated with SSEP functions.
- This licensee strives to reduce spare parts by interchanging common parts and components thus reducing inventory requirements and cost. Therefore the licensee uses multiple common parts and components in both SSEP and non-SSEP systems.
- Because the licensee interchanges the components and because some of the components are used in SSEP associated systems, the licensee protects all common parts for both SSEP and non-SSEP systems as CDAs such that the integrity of the components are maintained.
- The device has portable USB drives and only personnel who have been determined trustworthy in accordance with 10 CFR 73.56 and have a need for access, are granted access to the HMIs.
- Because of the limited nature of the operating system and communication protocols on this system and modules, an IDS would not be supported.
- This system is protected by and behind a one-way deterministic boundary device with no bypasses. The system modules functionality is firmware based requiring physical access and the system to be taken off line to change its functionality.

Detection along the threat pathway includes:

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable media__X__

IDS (HIDS/NIDS) ___

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	The system is not capable of supporting and IDS. Software changes are tested against signature and anomaly based indicators. PMD control program will detect malware on portable media and devices. Access control for HMI/keyboard, and critical values are checked.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators .
Does the licensee use whitelisting if technically possible?	Yes	System does not support whitelisting. CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee	Yes	The system does not support IDS or AV and as a result, signature based detection

update the signature indicators within (frequency)?		is not technically possible. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software. PMD control program will detect use signature based indicators to detect malware on portable media and devices.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indication is not supported by this system. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious, anomalous behavior, and unneeded software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. Operators monitor these systems 24/7 and will be able to detect anomalous behavior in plant equipment.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is not supported on installed equipment.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.

respond to cyber- attack alarm conditions?		
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.12 EXAMPLE 12: MICROPROCESSOR BASED I&C SYSTEM EXAMPLE B

Background

- Distributed Control System (DCS) was installed to address equipment obsolescence of the Westinghouse NSSS control system. The DCS is not safety-related and it controls the operation of the secondary side plant systems for feedwater, steam generator level, etc.
- The DCS includes a lot of connections to field devices for both input to the control processes and for output to control the plant equipment response for the given power conditions.
- A network connection is provided to the plant computer to provide information to plant personnel for monitoring of the DCS and plant parameters.
- Upgraded system was designed to be cyber security compliant with the licensee cyber security program, which was developed for NEI 04-04.
- An intrusion detection system (IDS) function and security information and event management (SIEM) function was included in the DCS.
- Whitelisting was not included in to the upgraded system.
- No wireless capabilities are included in the Distributed Control System
- Equipment cabinet access controlled through the key control program and work management processes
- PMMD program used to ensure secure connections with removable media
- Software controls included in the vendor activities for software requirement development, software design, and software testing. Vendor has software quality program and testing capabilities.
- Insider mitigation program used to ensure trust worthy individuals work on the system. Work performed using plant procedures by plant maintenance workers.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	System has IDS and a SIEM, which monitors connections within the plant LAN that is the interfacing system between the plant computer and the other plant digital control and monitoring systems. Any changes to the processor

		configuration or to the software will be performed by the design change process, which includes requirements for design development (hardware and software), testing, and installation. The licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible. Changes to system software will require design and testing by the vendor or software developer to ensure no unexpected software code is provided with a change.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee	Yes	Signature-based detection indicators are updated as required.

update the signature indicators within (frequency)?		
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indictors are accomplished as part of the App E section 11 System and Services Acquisition program. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, and installation. Operators also monitor plant other confirmatory plant equipment 24/7 and will identify anomalous equipment behavior.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is capable of detecting changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		

Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.13 EXAMPLE 13: MICROPROCESSOR BASED I&C SYSTEM EXAMPLE C

Background

- System utilizes Anti-Virus, HIDS, and Data Loss Prevention Protection.
- System contains several windows based computers and a number of firmware based components.
- System performs both indication and control functions.
- NIDS is deployed in accordance with defensive strategy at the network boundary.
- Logs are sent to the SIEM for analysis and alerting.
- Vendors without UAA must be escorted while in the plant and while working on the system.
- System does not utilize whitelisting.
- The SIEM deployed in accordance with procedure requirements provides mechanisms to identify and notify individuals of abnormal cyber conditions on the system. Notifications of events identified by the SIEM are forwarded to on call cyber analysts.
- The SIEM collects logs from systems, which support log forwarding.
- Network intuition detection servers monitor communications at the defensive level boundary and notify the on call cyber security analyst of events matching signatures.
- Plant Operators are trained to detect abnormal operation of the equipment and validate inputs using diverse methods.
- This equipment is located in locked cabinets with key control. Some cabinets are alarmed, with a trouble alarm sent to the control room via the PPC to detect unauthorized entry. Most of the equipment is located in the VA.
- Centrally managed Antivirus, Data loss prevention and HIDS software is deployed and monitored by SIEM to detect and prevent malicious software or unauthorized PMD use.
- PMD control provides adequate protection to mitigate and detect the PMD attack vector.
- Procurement of devices in accordance with System and Services Acquisition cyber security controls.

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection	Yes	System utilizes Anti-Virus, HIDS, and

capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?		Data Loss Protection. System contains several windows based computers and a number of firmware based components. NIDS is deployed in accordance with defensive strategy at the network boundary. Logs are sent to the SIEM for analysis and alerting. The licensee implements the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. PMD control program will detect malware on portable media and devices.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards on detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	Whitelisting is not technically possible because the system is a legacy system and is not supported anymore and the system may become unstable with whitelisting installed.

		Changes to system software will require design and testing by the vendor or software developer to ensure no unexpected software code is provided with a change.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	Signature-based detection indicators are updated as required.
Adequacy of anomaly based detection		
Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	The licensee uses anomaly indicators as part of its detection strategy and updates the anomaly indicators as needed. Anomaly indictors are also accomplished as part of the App E section 11 System and Services Acquisition program. Any changes to the processor configuration or to the software will be performed by the design change process which includes requirements for design development (hardware and software), testing, and installation. Operators monitor plant other confirmatory plant equipment 24/7 and will identify anomalous equipment behavior.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	The IDS is configured to detect unauthorized changes to itself.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response	Yes	The licensee uses onsite or on call 24/7 duty analyst and CSIRT for monitoring

support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?		and response and the Corporate SOC as backup. Personnel are trained to training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		
Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.

5.14 EXAMPLE 14: TRANSMITTER

This transmitter is a fully functional system within the scope of the CSP as a Direct CDA in accordance NEI 13-10. System attributes include:

- This remote transmitter is a flow transmitter used to modulate a flow control valve via the Distributed Control System (DCS) associated with an SSEP System. This is located within the PA and VA.
- The attack pathways to this device are by way of Maintenance and Test Equipment (MTE) and the data bus (4-20mA loop) and the supply chain.
- This device is protected by and behind a one-way deterministic boundary device with no bypasses.
- The device functionality is firmware based requiring physical access to change its functionality, however certain configuration parameters are manageable via the data bus.

Where along the attack pathway will the licensee detect a cyber attack?

Supply Chain_X__

External (Internet) Boundary Devices_____

Portable media__X__

IDS (HIDS/NIDS) ___

Access Control_X__

Wireless___

Operator __X___

IMP__X__

What is the licensee's strategy for implementing DRE?

Timely Attack Detection	Answer	Discussion
Did the licensee place its detection capability along the attack pathway, at a location where it can detect, respond and eliminate cyber attacks before adverse impact to the SSEP function?	Yes	To address detection, the licensee will implement the supply chain pathway detection, adequate implementation of NEI 08-09 Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious software and ensure control of devices and products when transmitted/transported to the site, and that

		positive control of the equipment is maintained. Software changes are verified against signature and anomaly based indicators. PMD control program will detect malware on portable devices.
Are personnel responsible for cyber–attack detection, trained in accordance with licensee training standards and are they sensitive to the indications of a cyber attack?	Yes	Personnel are trained in accordance with licensee training strategies and procedures.
Adequate detection:		
Adequacy of detection		
Are responders trained in accordance with licensee training standards on detection indicators?	Yes	Responders are trained IAW licensee standards of detection indicators.
Does the licensee use whitelisting if technically possible?	Yes	System does not support whitelisting. CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software. This is equivalent to whitelisting.
Adequacy of signature based detection		
If a signature-based detection is a technically possible approach to the detection strategy, does the licensee update the signature indicators within (frequency)?	Yes	The system does not support IDS or AV and as a result, signature based detection is not technically possible. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious and unneeded software. PMD control program will detect use signature based indicators to detect malware on portable media and devices.
Adequacy of anomaly based detection		

Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators with (frequency)?	Yes	Anomaly indication is not supported by this system. However, CSP implemented Appendix E Section 11 System and Services Acquisition controls will ensure testing and detection and elimination of malicious, anomalous behavior, and unneeded software and ensure control of devices and products when transmitted/transported to the site, and that positive control of the equipment is maintained. Operators monitor these systems 24/7 and will be able to detect anomalous behavior of plant equipment.
Integrity of the Intrusion Detection System		
If automatic IDS is used, is the IDS capable of detecting unauthorized changes to itself?	Yes	IDS is not supported on installed equipment, but is supported in equipment used a part of supply chain and acquisition equipment used to ensure adequate testing prior to being installed in plant systems.
Timely Adequate response, assessment and elimination:		
Determining ability		
Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response (on–site or on call), or use an off-site cyber security operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyber- attack alarm conditions?	Yes	The licensee uses a Corporate SOC as the 24/7 monitoring as well as onsite duty analyst and CSIRT for monitoring and response. Personnel are trained IAW licensee training standards.
Does the licensee have trained personnel, in accordance with licensee training standards, to assess and conduct an initial response to cyber attack alarm conditions?	Yes	Licensee personnel are appropriately trained to assess and conduct an initial response, in accordance with training standards.
Determining adequacy of personnel response.		

Are personnel responsible for response to cyber attacks trained, in accordance with licensee training standards, and sensitive to indications of a cyber attack?	Yes	Licensee personnel are trained to be sensitive to indications of cyber attack in accordance with training standards.
Are procedures exercised and tested?	Yes	Licensee routinely performs tabletop exercises and drills to test and exercise procedures.
Is the equipment the personnel use for response available to them?	Yes	Equipment is routinely checked to ensure available and operational in accordance with licensee maintenance procedures.
Is the environment the personnel respond in adequate to successful response?	Yes	Environment has been assessed in accordance licensee procedures.
Prevention of adverse impact to the SSEP function		
Determining adequacy of elimination		
Has the licensee developed procedures for response and elimination of the cyber attack threat relative to the CS?	Yes	Procedure have been developed and implemented.
Are personnel responsible for onsite response trained in accordance with licensee training standards procedures?	Yes	Personnel are trained in response in accordance with licensee procedures developed using training standards.