NRC FORM 464 Part I (03-2017) | U.S. NUCLEAR REGULATORY COMMISSION

RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) REQUEST

FOIA	RESPONSE NUMBER
2017-0674	1

RESPONSE TYPE ☐ INTERIM ☑ FINAL

REQUESTER:	DATE:
Diane Turco	10/06/2017

DESCRIPTION OF REQUESTED RECORDS:

Pilgrim Nuclear Power Station, "The Problem Identification and Resolution Sample Inspection Report 05000293/2017405"

PART I. -- INFORMATION RELEASED

You have the right to seek assistance from the NRC's FOIA Public Liaison. Contact information for the NRC's FOIA Public Liaison is available at https://www.nrc.gov/reading-rm/foia/contact-foia.html

- ☐ Agency records subject to the request are already available on the Public NRC Website, in Public ADAMS or on microfiche in the NRC Public Document Room.
- ☑ Agency records subject to the request are enclosed.
- ☐ Records subject to the request that contain information originated by or of interest to another Federal agency have been referred to that agency (see comments section) for a disclosure determination and direct response to you.
- ☐ We are continuing to process your request.
- ☑ See Comments.

PART I.A -- FEES

AMOUNT*

*See Comments for details

- ☐ You will be billed by NRC for the amount listed.
- ☐ You will receive a refund for the amount listed.
- ☐ Fees waived.

NO FEES

- ☑ Minimum fee threshold not met.
- ☐ Due to our delayed response, you will not be charged fees.

PART I.B -- INFORMATION NOT LOCATED OR WITHHELD FROM DISCLOSURE

- ☐ We did not locate any agency records responsive to your request. *Note*: Agencies may treat three discrete categories of law enforcement and national security records as not subject to the FOIA ("exclusions"). 5 U.S.C. 552(c). This is a standard notification given to all requesters; it should not be taken to mean that any excluded records do, or do not, exist.
- ☑ We have withheld certain information pursuant to the FOIA exemptions described, and for the reasons stated, in Part II.
- ☐ Because this is an interim response to your request, you may not appeal at this time. We will notify you of your right to appeal any of the responses we have issued in response to your request when we issue our final determination.
- ☑ You may appeal this final determination within 90 calendar days of the date of this response by sending a letter or e-mail to the FOIA Officer, at U.S. Nuclear Regulatory Commission, Washington, D.C. 20555-0001, or FOIA.Resource@nrc.gov. Please be sure to include on your letter or email that it is a "FOIA Appeal." You have the right to seek dispute resolution services from the NRC's Public Liaison, or the Office of Government Information Services (OGIS). Contact information for OGIS is available at https://ogis.archives.gov/about-ogis/contact-information.htm

PART I.C COMMENTS (Use attached Comments continuation page if required)

The NRC's letter transmitting the enclosed [redacted] report may be found in public ADAMS as ML17244A109. Records with an ML Accession Number are publicly available in the NRC's Public Electronic Reading Room at http:www.nrc.gov/reading-rm.html. If you need assistance in obtaining these records, please contact the NRC's Public Document Room (PDR) at 301-415-4737, or 1-800-397-4209, or by email to PDR.Resource@nrc.gov.

Signature - Freedom of Information Act Officer or Designee

Nina Argent

Digitally signed by Nina Argent
DN: c=US, o=U.S. Government, ou=U.S. Nuclear Regulatory Commission, ou=NRC-SW, cn=Nina Argent, 0.9.2342.19200300.100.1.1=200013425
Date: 2017.10.06 14:30:57 -04'00'

NRC FORM 464 Part II
(03-2017)

U.S. NUCLEAR REGULATORY COMMISSION

RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) REQUEST

FOIA: 2017-0674

DATE: 10/06/2017

PART II.A -- APPLICABLE EXEMPTIONS

Records subject to the request are being withheld in their entirety or in part under the FOIA exemption(s) as indicated below (5 U.S.C. 552(b)).

- ☐ Exemption 1: The withheld information is properly classified pursuant to an Executive Order protecting national security information.
- ☐ Exemption 2: The withheld information relates solely to the internal personnel rules and practices of NRC.
- ☐ Exemption 3: The withheld information is specifically exempted from public disclosure by the statute indicated.
  - ☐ Sections 141-145 of the Atomic Energy Act, which prohibits the disclosure of Restricted Data or Formerly Restricted Data (42 U.S.C. 2161-2165).
  - ☐ Section 147 of the Atomic Energy Act, which prohibits the disclosure of Unclassified Safeguards Information (42 U.S.C. 2167).
  - ☐ 41 U.S.C. 4702(b), which prohibits the disclosure of contractor proposals, except when incorporated into the contract between the agency and the submitter of the proposal.
- ☐ Exemption 4: The withheld information is a trade secret or confidential commercial or financial information that is being withheld for the reason(s) indicated.
  - ☐ The information is considered to be proprietary because it concerns a licensee's or applicant's physical protection or material control and accounting program for special nuclear material pursuant to 10 CFR 2.390(d)(1).
  - ☐ The information is considered to be another type or confidential business (proprietary) information.
  - ☐ The information was submitted by a foreign source and received in confidence pursuant to 10 CFR 2.390(d)(2).
- ☐ Exemption 5: The withheld information consists of interagency or intraagency records that are normally privileged in civil litigation.
  - ☐ Deliberative process privilege.
  - ☐ Attorney work product privilege.
  - ☐ Attorney-client privilege.
- ☐ Exemption 6: The withheld information from a personnel, medical, or similar file, is exempted from public disclosure because its disclosure would result in a clearly unwarranted invasion of personal privacy.
- ☑ Exemption 7: The withheld information consists of records compiled for law enforcement purposes and is being withheld for the reason(s) indicated.
  - ☐ (A) Disclosure could reasonably be expected to interfere with an open enforcement proceeding.
  - ☐ (C) Disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy.
  - ☐ (D) The information consists of names and other information the disclosure of which could reasonably be expected to reveal identities of confidential sources.
  - ☐ (E) Disclosure would reveal techniques and procedures for law enforcement investigations or prosecutions, or guidelines that could reasonably be expected to risk circumvention of the law.
  - ☑ (F) Disclosure could reasonably be expected to endanger the life or physical safety of an individual.
  - ☐ Other

PART II.B -- DENYING OFFICIALS

In accordance with 10 CFR 9.25(g) and 9.25(h) of the U.S. Nuclear Regulatory Commission regulations, the official(s) listed below have made the determination to withhold certain information responsive to your request.

DENYING OFFICIAL	TITLE/OFFICE	RECORDS DENIED	APPELLATE OFFICIAL	
			EDO	SECY
Nina E. Argent	Acting FOIA Officer	security-related information	☑	☐
			☐	☐
			☐	☐

Appeals must be made in writing within 90 calendar days of the date of this response by sending a letter or email to the FOIA Officer, at U.S. Nuclear Regulatory Commission, Washington, D.C. 20555-0001, or FOIA.Resource@nrc.gov. Please be sure to include on your letter or email that it is a "FOIA Appeal."

U. S. NUCLEAR REGULATORY COMMISSION

REGION I

Docket No.	50-293
License No.	DPR-35
Report No.	05000293/2017405
Licensee:	Entergy Nuclear Operations, Inc. (Entergy)
Facility:	Pilgrim Nuclear Power Station (Pilgrim)
Location:	600 Rocky Hill Road Plymouth, MA 02360
Dates:	June 5 - 8, 2017 July 5 – 7, 2017 August 7 - 11, 2017
Inspectors:	L. Dumont, Reactor Inspector
Approved by:	Glenn T. Dentel, Chief Engineering Branch 2 Division of Reactor Safety

Enclosure

SUMMARY

IR 05000293/2017405; 06/05/2017 – 06/08/2017, 07/05/2017 – 07/07/2017, 08/07/2017 – 08/11/2017; Pilgrim; Problem Identification and Resolution.

The report covered a cyber security problem identification and resolution sample inspection by a region-based inspector. Two NRC-identified findings were identified. These findings were discussed and reviewed during the Security Issues Forum meeting conducted on July 27, 2017. The significance of most findings is indicated by their color (i.e., greater than Green, or Green, White, Yellow, Red) using Inspection Manual Chapter (IMC) 0609, "Significance Determination Process," dated April 29, 2015. Cross-cutting aspects are determined using IMC 0310, "Aspects Within the Cross-Cutting Areas," dated December 4, 2014. All violations of NRC requirements are dispositioned in accordance with the NRC's Enforcement Policy, dated November 1, 2016. The NRC's program for overseeing the safe operation of commercial nuclear power reactors is described in NUREG-1649, "Reactor Oversight Process," Revision 6, dated July 2016.

A. NRC-Identified Findings

Cornerstone: Physical Security

- Green. The inspector identified a finding of very low cyber security significance (Green) involving a non-cited violation (NCV) of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(b)(10), for the failure to perform adequate corrective actions (b)(7)(F) Entergy entered these issues into their corrective action program (CAP) as condition reports (CRs) (PNP-2017-05997, 06020, 06035, 06047, 06050, and 06191).

  This finding was more than minor because it was associated with the (b)(7)(F) The inspector evaluated the finding in accordance with NRC IMC 0609, "Significance Determination Process," Appendix E, Part IV, "Cyber Security Significance Determination Process," and determined that (b)(7)(F) As a result, this finding was determined to be of very low safety significance (Green). This finding had a cross-cutting aspect in the area of Problem Identification and Resolution, specifically Resolution, because Entergy did not take effective corrective action to resolve and correct a previous NRC-identified violation for the failure to (b)(7)(F) [P.3] (Section 4OA2)

- Green. The inspector identified a violation of very low safety significance (Green) involving an NCV of 10 CFR 73.55(b)(4), for the failure to perform adequate analysis of site specific conditions, including target sets. Specifically, Entergy (b)(7)(F)

  This finding was more than minor because it was associated with the Response to Contingency Events (Implementation of the Protective Strategy) attribute of the Security cornerstone, and it adversely affected the cornerstone objective to provide assurance that the licensee's security system could protect against the design basis threat of radiological sabotage from external threats. Specifically, (b)(7)(F) The inspector evaluated the finding in accordance with IMC 0609, "Significance Determination Process," Appendix E, Part I, "Baseline Security Significance Determination Process for Power Reactors." The inspector determined that the negative impact the performance deficiency had on the probability of physical protection effectiveness was very low, because the modification did not require the licensee to make any changes to their protective strategy. As a result, this finding was determined to be of very low safety significance (Green). This finding had a cross-cutting aspect in the area of Problem Identification and Resolution, Evaluation, because Entergy did not adequately evaluate their (b)(7)(F) [P.2] (Section 4OA2)

B. Other Findings

None.

REPORT DETAILS

Background

During 2013 through 2015, the NRC performed a programmatic review of each licensee's implementation of the their cyber security program to assess and verify that interim Milestones 1 through 7 of the licensee's cyber security program implementation schedule had been adequately completed in accordance with the regulatory requirements of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," the licensee's CSP, and NRC approved implementation schedules.

4. OTHER ACTIVITIES [OA]

4OA2 Identification and Resolution of Problems (71152 - 1 sample)

a. Inspection Scope

The inspector performed an in-depth review of Entergy's evaluations and corrective actions for findings previously identified during the conduct of Temporary Instruction (TI) 2201/004 at Pilgrim. Four NRC-identified findings were documented for Milestone 2, 3, 4, and 6. The inspector specifically reviewed issues associated with these four Milestones within the scope of this inspection.

The inspector assessed Entergy's problem identification threshold, problem analyses, extent of condition reviews, compensatory actions, and the prioritization and timeliness of corrective actions to determine whether Entergy was appropriately identifying, characterizing, and correcting problems associated with the NRC-identified findings identified during the TI 2201/004 inspection, and whether the planned or completed corrective actions were appropriate. The inspector compared the actions taken to the requirements of Entergy's CAP and the facility CSP.

The inspector reviewed cyber security records and implementing program procedures, and interviewed cyber security, physical security, engineering, and operations personnel to assess the effectiveness of the implemented corrective actions, the reasonableness of the planned corrective actions, and to evaluate the extent of any ongoing problems.

Milestone 2: Identification & Documentation of Critical Systems & Critical Digital Assets

Milestone 2 required licensees to identify and document critical systems and CDAs as described in CSP Section 3.1.3, "Identification of Critical Digital Assets." These systems and digital assets included digital computer and communication systems and networks associated with safety-related and important to safety functions, security functions, emergency preparedness functions (including off-site communications), and support systems and equipment which, if compromised, would adversely impact SSEP functions. These systems and assets also included additional structures, systems, and components that have a nexus to radiological health and safety and therefore can directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient.

Milestone 3: Installation of a Protective Device between Lower & Higher Security Levels

Milestone 3 required licensees to install deterministic one-way devices (e.g., data diodes) between computer networks at a lower security level (i.e., levels 0, 1, and 2) and a higher security level (i.e., levels 3 and 4), as described in CSP Section 4.3, "Defense-In-Depth Protective Strategies." Any lower security level device that bypassed the deterministic device and connected to level 3 or 4 were required to be modified to eliminate the bypass, or modified to meet cyber security requirements commensurate with the higher security level network to which they connect. Milestone 3 also required that any design modification not completed by the required interim implementation date be documented in the site configuration management and change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.

Milestone 4: Implementation of Access Control for Portable and Mobile Devices

Milestone 4 required licensees to implement technical security controls for portable and mobile devices as described in Appendix D, Section 1.19, "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6. Those controls, in part, requires the licensee to establish and document usage restrictions and implementation guidance for controlled portable and mobile devices; authorize, monitor, and control device access to CDAs; enforce and document mobile device security and integrity at a level consistent with the CDA they support; and enforce and document that mobile devices are used in one security level and are not moved between security levels.

Milestone 6: Implementation of Cyber Security Controls for Critical Digital Assets that could Adversely Impact the Design Function of Target Set Equipment

Milestone 6 required licensees to identify, document, and implement technical cyber security controls for CDAs that could adversely impact the design function of physical security target set equipment in accordance with CSP Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls." CSP Section 3.1.6 required licensees to establish defense-in-depth strategies for CDAs by implementing the recommendations described in Appendix D, "Technical Cyber Security Controls," and Appendix E, "Operational and Management Cyber Security Controls," of NEI 08-09, Revision 6. The technical cyber security controls were intended to provide a high degree of protection against cyber-related attacks. A security control was considered to be applied when there was high assurance that the CDA's safety or security function would not be adversely impacted by the implemented security control. When a cyber security control was determined to have an adverse effect, alternate controls were required to protect the CDA. Milestone 6 also required that any design modification not completed by the required interim implementation date, be documented in the site configuration management and change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.

Specific documents reviewed by the inspector are listed in the Attachment to this report.

b. Findings

Failure to Complete Milestone 2 Corrective Actions to Identify Critical Digital Assets

Introduction. The inspector identified a finding of very low cyber security significance (Green) involving an NCV of 10 CFR 73.55(b)(10), for the failure to perform adequate corrective actions in the identification of CDAs. Specifically, Entergy had a corrective action to identify and document CDAs in accordance with Pilgrim's CSP Section 3.1.3, "Identification of Critical of Digital Assets," but failed to identify and document 23 digital assets, which performed safety-related, important to safety and emergency preparedness functions, as CDAs.

Description. The inspector reviewed corrective actions from several CRs associated with Milestone 2 issues and the Milestone 2 NRC-identified finding documented in NRC Inspection Report 05000293/2015403. On June 6, 2017, the inspector reviewed Pilgrim's Non-CDA Digital Devices list and identified

(b)(7)(F)

Entergy entered these issues into their CAP as CRs (PNP-2017-05997, 06020, 06035, 06047, 06050, and 06191).

Analysis. Entergy's failure to adequately perform planned corrective actions to resolve a previous NRC-identified violation was a performance deficiency. This performance deficiency was a failure to adequately identify and document CDAs in accordance with Pilgrim's CSP Section 3.1.3, "Identification of Critical of Digital Assets."

This finding was more than minor because it was associated with the Response to Contingency Events attribute of the Security cornerstone and adversely affected the cornerstone's objective to provide assurance that a licensee's protective strategy can protect against design basis threats of radiological sabotage from external and internal threats. Specifically, (b)(7)(F)

The inspector evaluated the finding in accordance with NRC IMC 0609, "Significance Determination Process," Appendix E, Part IV, "Cyber Security Significance Determination Process." The inspector determined that (b)(7)(F) As a result, this finding was determined to be of very low safety significance (Green) ("No" to Figure 1, Step 2).

This finding had a cross-cutting aspect in the area of Problem Identification and Resolution, specifically Resolution, because Entergy did not take effective corrective actions to resolve and correct a previous NRC-identified violation for the failure to identify digital assets associated with critical systems as CDAs. [P.3]

Enforcement. 10 CFR 73.55, "Physical Protection against Radiological Sabotage," subpart (b)(10), in part, required Entergy to use the site CAP to correct deficiencies in the physical protection program. The cyber security program is a component of the physical protection program as described in 10 CFR 73.54(b)(3). Contrary to the above, from January 28, 2015, to present, Entergy (b)(7)(F) as documented in NRC Inspection Report 05000293/2015403. The NRC is treating this violation as an NCV, consistent with Section 2.3.2.a of the NRC Enforcement Policy, because this finding was of very low safety significance (Green) and was entered into Entergy's CAP (CR-PNP-2017-05997,06020, 06035, 06047, 06050, and 06191). **(NCV 05000293/2017405-01, Failure to Complete Milestone 2 Corrective Actions to Identify Critical Digital Assets)**

Failure to Adequately Analyze Target Sets and Mitigate Vulnerabilities that could Impact the Design Function of target set equipment

Introduction. The inspector identified a violation of very low safety significance (Green) involving an NCV of 10 CFR 73.55(b)(4), for the failure to perform adequate analysis of site specific conditions, including target sets. Specifically (b)(7)(F)

(b)(7)(F)

Description. During Pilgrim's last TI 2201/004 inspection, the NRC identified

(b)(7)(F)

Analysis. The inspector determined that the failure to perform an adequate analysis of site specific conditions, including target sets, in accordance with 10 CFR 73.55(b)(4) was a performance deficiency because Entergy failed to meet a regulatory requirement that was reasonably within its ability to foresee and correct and should have been prevented. Traditional enforcement does not apply because the issue did not have any actual security consequences or potential for impacting the NRC's regulatory function and was not the result of any willful violation of NRC requirements or Entergy procedures.

The performance deficiency was more than minor because it was associated with the Response to Contingency Events (Implementation of the Protective Strategy) attribute of the Security cornerstone, and it adversely affected the cornerstone objective to provide assurance that the licensee's security system could protect against the design basis threat of radiological sabotage from external threats. Specifically,

(b)(7)(F)

The inspector evaluated the finding in accordance with IMC 0609, "Significance Determination Process," Appendix E, Part I, "Baseline Security Significance Determination Process for Power Reactors." Figure 1, Baseline Security Significance Determination Processs Flowchart, directed the inspector to Figure 4, Significance

Screen Process, since all findings related to target sets meet the significance screen criteria for physical protection. The inspector determined that the negative impact the performance deficiency had on the probability of physical protection effectiveness was very low, because the modification did not require the licensee to make any changes to their protective strategy. As a result, this finding was determined to be of very low safety significance (Green) (probability matrix was very low on Figure 4, Step 4). This finding had a cross-cutting aspect in the area of Problem Identification and Resolution, Evaluation, because Entergy did not adequately evaluate their

(b)(7)(F)

Enforcement. 10 CFR 73.55(b)(4) requires the licensee, in part, to analyze site specific condition, including target sets, that may affect the specific measures needed to implement the requirements of physical protection. Contrary to the above, on

(b)(7)(F)

The NRC is treating this violation as an NCV, consistent with Section 2.3.2.a of the NRC Enforcement Policy, because this finding was of very low safety significance (Green) and was entered into Entergy's CAP. **(NCV 05000293/2017405-02, Failure to Adequately Analyze Target Sets and Mitigate Vulnerabilities that could Impact the Design Function of Target Set Equipment)**

4OA6 Meetings, Including Exit

Exit Meeting Summary

The inspector presented the preliminary inspection results to Mr. Franco Pasquale, Information Technology Manager, and other members of Entergy's staff on August 23, 2017. The inspector verified that no proprietary information was included in this report.

ATTACHMENT: SUPPLEMENTARY INFORMATION

SUPPLEMENTARY INFORMATION

KEY POINTS OF CONTACT

Licensee Personnel

R. Byrne, Regulatory Assurance
M. Boucher, IT Specialist
G. Cassell, Lead Facility and Equipment Specialist
N. Eisenman, Engineering/System Supervisor
M. Gatslick, Senior Security Supervisor
G. McDonald, I&C Technician
J. Odonnell, System engineer
F. Pasquale, IT Manager
J. Webers, Operations Work Liaison
C. Wilson, Senior IT Consultant

NRC Personnel
E. Carfang, Senior Resident Inspector, Pilgrim
B. Pinson, Resident Inspector, Pilgrim
J. Bream, Physical Security Inspector
S. McCarver, Physical Security Inspector

LIST OF ITEMS OPENED, CLOSED, AND DISCUSSED

Opened

None.

Opened and Closed

05000293/2017405-01	NCV	Failure to Complete Milestone 2 Corrective Actions to Identify Critical Digital Assets (Section 4OA2)
05000293/2017405-02	NCV	Failure to Adequately Analyze Target Sets and Mitigate Vulnerabilities that could Impact the Design Function of Target Set Equipment (Section 4OA2)

Closed

None.

Attachment

LIST OF DOCUMENTS REVIEWED

Licensing and Design Basis Documents
Pilgrim Nuclear Power Station Cyber Security Plan, Revision 001
Attachment 1 to PNPS letter 2.11.016, Response to Request for Additional Information

Procedures
EN-EP-202, Equipment Important to Emergency Preparedness, Revision 1
EN-FAP-IT-009, Nuclear Cyber Security Terms and Definitions, Revision 4
EN-IT-103, Nuclear Cyber Security Program, Revision 12
EN-IT-103-01, Control of Portable Media Connected to Critical Digital Assets, Revision 11
EN-IT-103-03, Cyber Security Assessment Process, Revision 1
EN-IT-103-04, Critical Digital Asset Technical Control Requirements, Revision 0
EN-LI-102, Corrective Action Program, Revision 29
EN-MA-105, Control of Measuring and Test Equipment (M&TE), revision 13
EN-NS-306, Development and Maintenance of Critical Target sets, Revision 4
EP-AD-270, Equipment Important to Emergency Response (EITER), Revision 3

Drawings, and Piping and Instrumentation Diagrams
M226A5, Elementary Diagram Emergency& Plant Information Computer System (EPIC) Switch Connections C940-72, Revision 6
M226A6, Elementary Diagram Emergency& Plant Information Computer System (EPIC) Bridge (BTEB)/DAS Connections C940-73, Revision 5
M226A6 Sheet 2, Elementary Diagram Emergency& Plant Information Computer System (EPIC) DAS/Switch Connections, Revision 0
M226A7, Elementary Diagram Emergency& Plant Information Computer Center, Revision 9
M226A8, Elementary Diagram Emergency& Plant Information Computer System, Revision 6
PNP network, PNP Switch Interconnect, Revision 16

Condition Reports (* denotes NRC identified during this inspection)

CR-PNP-2017-05959*	CR-PNP-2015-00601	CR-PNP-2015-01157
CR-PNP-2017-05997*	CR-PNP-2015-00650	CR-PNP-2015-00655
CR-PNP-2017-06020*	CR-PNP-2015-00585	CR-PNP-2015-00605
CR-PNP-2017-06034*	CR-PNP-2015-00620	CR-PNP-2015-00653
CR-PNP-2017-06035*	CR-PNP-2015-00644	CR-PNP-2015-00657
CR-PNP-2017-06047*	CR-PNP-2015-00698	CR-PNP-2015-00699
CR-PNP-2017-06050*	CR-PNP-2015-00128	CR-PNP-2015-00272
CR-PNP-2015-00508	CR-PNP-2015-00590	CR-PNP-2015-00617
CR-PNP-2015-00618	CR-PNP-2015-00618	CR-PNP-2015-00643
CR-PNP-2015-00651	CR-PNP-2017-04776	

Training Documents
EN-TQ-131, Nuclear Cyber Security Training & Qualification, Revision 0

Industry Standards
NRC Regulatory Guide 5.71, Cyber Security Programs, 1/2016
NEI 08-09, Cyber Security Plan for Nuclear Power Reactors, Revision 6
NEI 10-04, Identifying Systems and Assets Subject to the Cyber Security Rule, Revision 2

Miscellaneous Documents
2.16.045, Pilgrim Nuclear Power Station's Response to Cyber Security Inspection Report Identified Enforcement Discretion Violations, Dated 8/15/16
Kiosk Number 2 Maintenance Log from 4/12/17 to 5/31/17
Kiosk Number 3 Maintenance Log from 4/12/17 to 5/31/17
Kiosk Number 4 Maintenance Log from 4/12/17 to 5/31/17
MS Excel file of Critical Digital Asset Approved List, dated 5/10/17
MS Excel file Non-CDA Digital Devices List, dated 5/10/17
List of Critical Plant Systems, dated 5/10/17
List of Non-Critical Plant System, dated 5/10/17

LIST OF ACRONYMS

CAP	corrective action program
CDA	critical digital asset
CFR	*Code of Federal Regulations*
CR	condition report
CSP	Cyber Security Plan
IMC	Inspection Manual Chapter
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
NCV	non-cited violation
SSEP	safety, security, and emergency preparedness
TI	temporary instruction