NEXTera ENERGY
DUANE ARNOLD

~~SECURITY RELATED INFORMATION~~
~~WITHHOLD FROM PUBLIC DISCLOSURE UNDER 10 CFR 2.390~~

July 14, 2010

NG-10-0320
10 CFR 50.90
10 CFR 50.4

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

Duane Arnold Energy Center
Docket No. 50-331
License No. DPR-49

License Amendment Request (TSCR-121A): Request for Approval of the Duane Arnold Energy Center/NextEra Energy Duane Arnold, LLC Cyber Security Plan

References:

(1) Letter from NextEra Energy Duane Arnold to NRC, "License Amendment Request (TSCR-121): Request for Approval of the Duane Arnold Energy Center/NextEra Energy Duane Arnold, LLC Cyber Security Plan," dated November 19, 2009. (ML093270073)

(2) Letter from NextEra Energy Duane Arnold to NRC, "Revision to No Significant Hazards Consideration for License Amendment Request (TSCR-121): Request for approval of the Duane Arnold Energy Center/NextEra Energy Duane Arnold, LLC Cyber Security Plan," dated January 13, 2010. (ML100190150)

(3) Letter from NRC to NextEra Energy Duane Arnold, "License Amendment Request for Approval of the Cyber Security Plan (TAC No. ME2705)," dated May 20, 2010. (ML101390323)

**Enclosure 3 to this letter contains sensitive information.**
**Withhold from public disclosure under 10 CFR 2.390.**
**Upon removal of Enclosure 3, this letter is decontrolled.**

In response to Reference 3, and in accordance with the provisions of 10 CFR 50.4 and 10 CFR 50.90, NextEra Energy Duane Arnold, LLC is hereby submitting a request for amendment to the Operating License (OL) for the Duane Arnold Energy Center (DAEC)/NextEra Energy Duane Arnold. This proposed amendment requests NRC approval of the NextEra Energy Duane Arnold Cyber Security Plan, provides an implementation schedule, and adds a sentence to the existing OL Physical Protection license condition to require NextEra Energy Duane Arnold to fully implement and maintain in effect all provisions of the Commission approved Cyber Security Plan. The Plan follows NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," with a few exceptions as described in Enclosure 1.

With this submittal NextEra Energy Duane Arnold withdraws its previous submittals, (Reference 1 and 2) that were based on a prior version of NEI 08-09 guidance.

Enclosure 1 of this submittal provides an evaluation of the proposed change and contains the following attachments:

- Attachment 1 provides the existing OL page marked up to show the proposed change.
- Attachment 2 provides the proposed OL changes in final typed format.

Enclosure 2 provides a copy of the DAEC/NextEra Energy Duane Arnold Cyber Security Plan Implementation Schedule that contains milestones which are identified as commitments.

Enclosure 3 provides a copy of the DAEC/NextEra Energy Duane Arnold, LLC Cyber Security Plan which is a stand alone document that will be incorporated by reference into the DAEC/NextEra Energy Duane Arnold Physical Security Plan after approval. NextEra Energy Duane Arnold requests that Enclosure 3, which contains sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390(d)(1).

This application has been reviewed by the NextEra Energy Duane Arnold Onsite Review Group. The proposed amendment presents no significant hazards consideration under the standards set forth in 10 CFR 50.92(c). A copy of this submittal, along with the 10 CFR 50.92 evaluation of "No Significant Hazards Consideration," is being forwarded to our appointed state official pursuant to 10 CFR 50.91.

**Enclosure 3 to this letter contains sensitive information.**
**Withhold from public disclosure under 10 CFR 2.390.**
**Upon removal of Enclosure 3, this letter is decontrolled.**

NextEra Energy Duane Arnold requests an implementation date of December 31, 2014 based upon the enclosed implementation schedule. If you should have any questions or require additional information, please contact Steve Catron, Licensing Manager, at (319) 851-7234.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 14, 2010.

Christopher R. Costanzo
Vice President, Duane Arnold Energy Center
NextEra Energy Duane Arnold, LLC

Enclosure 1 – Evaluation of Proposed Change
Attachment 1 – Proposed Facility Operating License Change (Mark-up)
Attachment 2 – Proposed Facility Operating License Change (Re-typed)
Enclosure 2 – NextEra Energy Duane Arnold Cyber Security Plan Implementation Schedule
Enclosure 3 – Cyber Security Plan for Duane Arnold Energy Center (DAEC)/NextEra Energy Duane Arnold, LLC

cc: M. Rasmusson (State of Iowa)

**Enclosure 3 to this letter contains sensitive information.**
**Withhold from public disclosure under 10 CFR 2.390.**
**Upon removal of Enclosure 3, this letter is decontrolled.**

ENCLOSURE 1

EVALUATION OF PROPOSED CHANGE

SUBJECT: License Amendment Request (TSCR-121A): Request for Approval of the Duane Arnold Energy Center/NextEra Energy Duane Arnold, LLC Cyber Security Plan


1.0 SUMMARY DESCRIPTION
2.0 DETAILED DESCRIPTION
3.0 TECHNICAL EVALUATION
4.0 REGULATORY EVALUATION
    4.1 APPLICABLE REGULATORY REQUIREMENTS/CRITERIA
    4.2 SIGNIFICANT HAZARDS CONSIDERATION
    4.3 CONCLUSION
5.0 ENVIRONMENTAL CONSIDERATION
6.0 REFERENCES


---

ATTACHMENTS:
Attachment 1 – PROPOSED FACILITY OPERATING LICENSE CHANGE (MARK-UP)
Attachment 2 – PROPOSED FACILITY OPERATING LICENSE CHANGE (RE-TYPED)

## 1.0 SUMMARY DESCRIPTION

The proposed license amendment request (LAR) includes the proposed DAEC/NextEra Energy Duane Arnold Cyber Security Plan (Plan), an Implementation Schedule, and a proposed sentence to be added to the existing OL Physical Protection license condition.

## 2.0 DETAILED DESCRIPTION

The proposed LAR includes three parts: the proposed Plan, an Implementation Schedule, and a proposed sentence to be added to the existing OL Physical Protection license condition to require NextEra Energy Duane Arnold to fully implement and maintain in effect all provisions of the Commission approved Cyber Security Plan as required by 10 CFR 73.54. *Federal Register* notice 74 FR 13926 issued the final rule that amended 10 CFR Part 73. The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under Part 50 of this chapter to submit a cyber security plan that satisfies the requirements of the Rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's cyber security program must be consistent with the approved schedule. The background for this application is addressed by the NRC Notice of Availability published on March 27, 2009, 74 FR 13926 (Reference 1).

## 3.0 TECHNICAL EVALUATION

*Federal Register* notice 74 FR 13926 issued the final rule that amended 10 CFR Part 73. Cyber security requirements are codified as new 10 CFR 73.54 and are designed to 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 established by § 73.1(a)(1)(v). These requirements enhance upon the requirements imposed by EA-02-026 (Reference 2).

This LAR includes the proposed change to the existing OL license condition for "Physical Protection" (Attachments 1 and 2). In addition, the LAR contains the proposed Implementation Schedule (Enclosure 2) as required by 10 CFR 73.54. Finally, this LAR includes the proposed Plan (Enclosure 3) that conforms to the template provided in NEI 08-09 Revision 6, with the following exceptions:

Definition of cyber attack

In lieu of the use of the definition of “cyber attack” in NEI 08-09 Revision 6, the following definition of “cyber attack” will be used, “Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a Critical Digital Asset.” According to the June 7, 2010 letter to NEI (Reference 3), the NRC staff has found this definition to be acceptable.

Emergency preparedness
10 CFR 73.54 requires protecting digital computer and communication systems and networks associated with emergency preparedness (EP) functions, including offsite communications. The EP functions within the scope of the Plan are those functions which support implementation of the Risk Significant Planning Standards* (RSPSs) as defined in NRC Inspection Manual Chapter 0609, Appendix B. The RSPSs are the subset of EP Planning Standards, defined in 10 CFR 50.47(b), which play the greatest role in protecting public health and safety. In terms of importance, this approach aligns the selected EP functions with other system functions which are "Safety-Related" or "Important-to-Safety."

10 CFR 73.56(b)(ii) requires that any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's emergency preparedness be subject to an access authorization program. However, some systems, or portions of systems, which perform a RSPS-related EP function may be located in offsite locations not under the control of the licensee and/or not staffed by licensee personnel. Similarly, there may be system components that are normally installed, modified or maintained by non-licensee personnel (e.g., a telecommunications company technician, and employee of a State agency, etc.).

Therefore the systems, and portions of systems, to be protected from cyber attack in accordance with 10 CFR 73.54(a)(1)(iii) must;

1. Perform a RSPS-related EP function, and
2. Be within the licensee's complete custody and control.

* The RSPSs are 10 CFR 50.47(b)(4), (5), (9), and (10), including the related sections of Appendix E to 10 CFR Part 50. 10 CFR 50.47(b)(10) has two aspects that are of differing risk-significance. Only the portion dealing with the development of protective action recommendations (PARs) is integral to protection of public health and safety and is considered to be an RSPS.

Senior nuclear management
Senior nuclear management is defined as the Vice President accountable for nuclear plant security. The NEI 08-09 template defines this position as accountable for nuclear plant operation. The position of Vice President accountable for nuclear plant security better reflects the duties and responsibilities of the NextEra Energy Duane Arnold Cyber Security Plan.

## 4.0 REGULATORY EVALUATION

### 4.1 APPLICABLE REGULATORY REQUIREMENTS/CRITERIA

This LAR is submitted pursuant to 10 CFR 73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a Cyber Security Plan as specified in 10 CFR 50.4 and 10 CFR 50.90.

## 4.2 SIGNIFICANT HAZARDS CONSIDERATION

NextEra Energy Duane Arnold has evaluated whether or not a significant hazards consideration is involved with the proposed amendment by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of amendment," as discussed below:

1. Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No.

The proposed amendment incorporates a new requirement in the Facility Operating License to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. Inclusion of the Cyber Security Plan in the Facility Operating License itself does not involve any modifications to the safety-related structures, systems or components (SSCs). Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are to be implemented to identify, evaluate, and mitigate cyber attacks up to and including the design basis cyber attack threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks. The Cyber Security Plan will not alter previously evaluated Final Safety Analysis Report (FSAR) design basis accident analysis assumptions, add any accident initiators, or affect the function of the plant safety-related SSCs as to how they are operated, maintained, modified, tested, or inspected. Therefore, the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

The proposed amendment provides assurance that safety-related SSCs are protected from cyber attacks. Implementation of 10 CFR 73.54 and the inclusion of a plan in the Facility Operating License do not result in the need for any new or different FSAR design basis accident analysis. It does not introduce new equipment that could create a new or different kind of accident, and no new equipment failure modes are created. As a result, no new accident scenarios, failure mechanisms, or limiting single failures are introduced as a result of this proposed amendment. Therefore, the proposed amendment does not create a possibility for an accident of a new or different type than those previously evaluated.

3. Does the proposed amendment involve a significant reduction in a margin of safety?

Response: No.

The margin of safety is associated with the confidence in the ability of the fission product barriers (i.e., fuel cladding, reactor coolant pressure boundary, and containment structure) to limit the level of radiation to the public. The proposed amendment would not alter the way any safety-related SSC functions and would not alter the way the plant is operated. The amendment provides assurance that safety-related SSCs are protected from cyber attacks. The proposed amendment would not introduce any new uncertainties or change any existing uncertainties associated with any safety limit. The proposed amendment would have no impact on the structural integrity of the fuel cladding, reactor coolant pressure boundary, or containment structure. Based on the above considerations, the proposed amendment would not degrade the confidence in the ability of the fission product barriers to limit the level of radiation to the public. Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Based on the above, NextEra Energy Duane Arnold concludes that the proposed change presents no significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of no significant hazards consideration is justified.

## 4.3 CONCLUSION

In conclusion, based on the considerations discussed above, (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

## 5. 0 ENVIRONMENTAL CONSIDERATION

The proposed amendment establishes the licensing basis for a Cyber Security Program for DAEC and will be a part of the Physical Security Plan. This proposed amendment will not involve any significant construction impacts. Pursuant to 10 CFR 51.22(c)(12) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

## 6.0 REFERENCES

1. Federal Register Notice, Final Rule 10 CFR Part 73, "Power Reactor Security Requirements," published on March 27, 2009, 74 FR 13926.
2. EA-02-026, "Issuance of Order for Interim Safeguards and Security Compensatory Measures," issued February 25, 2002.

3. Letter to C. Earls, NEI from NRC, “Nuclear Energy Institute 08-09, “Cyber Security Plan Template, Rev. 6,”” dated June 7, 2010. (ML101550052)

ENCLOSURE 1

ATTACHMENT 1

PROPOSED FACILITY OPERATING LICENSE CHANGE

(MARK-UP)

2 Pages Follow

(a) For Surveillance Requirements (SRs) whose acceptance criteria are modified, either directly or indirectly, by the increase in authorized maximum power level in 2.C.(1) above, in accordance with Amendment No. 243 to Facility Operating License DPR-49, those SRs are not required to be performed until their next scheduled performance, which is due at the end of the first surveillance interval that begins on the date the Surveillance was last performed prior to implementation of Amendment No. 243.

(b) Deleted.

(3) Fire Protection

NextEra Energy Duane Arnold, LLC shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report for the Duane Arnold Energy Center and as approved in the SER dated June 1, 1978, and Supplement dated February 10, 1981, subject to the following provision:

NextEra Energy Duane Arnold, LLC may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

(4) The licensee is authorized to operate the Duane Arnold Energy Center following installation of modified safe-ends on the eight primary recirculation system inlet lines which are described in the licensee letter dated July 31, 1978, and supplemented by letter dated December 8, 1978.

(5) Physical Protection

NextEra Energy Duane Arnold, LLC shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Duane Arnold Energy Center Physical Security Plan," submitted by letter dated May 16, 2006.

INSERT A ⟶

*INSERT A*

*NextEra Energy Duane Arnold, LLC shall fully implement and maintain in effect all provisions of the Commission-approved Duane Arnold Energy Center/NextEra Energy Duane Arnold, LLC Cyber Security Plan submitted by letter dated July 14, 2010 and withheld from public disclosure in accordance with 10 CFR 2.390.*

ENCLOSURE 1

ATTACHMENT 2

PROPOSED FACILITY OPERATING LICENSE CHANGE

(RE-TYPED)

1 Page Follows

(a) For Surveillance Requirements (SRs) whose acceptance criteria are modified, either directly or indirectly, by the increase in authorized maximum power level in 2.C.(1) above, in accordance with Amendment No. 243 to Facility Operating License DPR-49, those SRs are not required to be performed until their next scheduled performance, which is due at the end of the first surveillance interval that begins on the date the Surveillance was last performed prior to implementation of Amendment No. 243.

(b) Deleted.

(3) Fire Protection

NextEra Energy Duane Arnold, LLC shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report for the Duane Arnold Energy Center and as approved in the SER dated June 1, 1978, and Supplement dated February 10, 1981, subject to the following provision:

NextEra Energy Duane Arnold, LLC may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

(4) The licensee is authorized to operate the Duane Arnold Energy Center following installation of modified safe-ends on the eight primary recirculation system inlet lines which are described in the licensee letter dated July 31, 1978, and supplemented by letter dated December 8, 1978.

(5) Physical Protection

NextEra Energy Duane Arnold, LLC shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: “Duane Arnold Energy Center Physical Security Plan,” submitted by letter dated May 16, 2006.

NextEra Energy Duane Arnold, LLC shall fully implement and maintain in effect all provisions of the Commission-approved Duane Arnold Energy Center/NextEra Energy Duane Arnold, LLC Cyber Security Plan submitted by letter dated July 14, 2010 and withheld from public disclosure in accordance with 10 CFR 2.390.

ENCLOSURE 2

NEXTERA ENERGY DUANE ARNOLD
CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE

4 Pages Follow

**NextEra Energy Duane Arnold**
**Cyber Security Plan Implementation Schedule**

Generic RAI Question # 29 includes reference to previous regulatory guidance and industry initiatives related to cyber security. As referenced, current industry guidance for cyber security is described in NEI 04-04, *Cyber Security Program for Power Reactors*. However, the scope of requirements in the NRC accepted implementation guidance contained in NEI 08-09 revision 6 are significantly greater than the previously implemented cyber security program. The defensive model design requirements, the new digital asset assessment methodology and the resultant digital asset remediation actions will require a significant expenditure of labor resources. As referenced in the Generic RAI Question # 29, NextEra Energy Duane Arnold is also required to implement a separate cyber security program in accordance with the NERC Critical Infrastructure Protection Standards. While the timeframe for implementation is shorter for the NERC regulation as described in the RAI question, the NERC cyber security methodology is different from the NRC Rule requirements. The NERC requirements are based on a logical risk based assessment process while the NRC Rule 73.54 requires a deterministic cyber security assessment methodology.

In light of the extensive work associated with implementation of these two new regulations, NextEra Energy Duane Arnold has developed a prioritized approach to establish the NRC Rule 73.54 implementation schedule. NextEra Energy Duane Arnold realizes the importance of deploying a uni-directional communication barrier to protect the most critical safety-related and important-to safety functions, security functions, and emergency preparedness functions including offsite communications (SSEP functions). One major activity is the deployment of uni-directional communication barrier to ensure protection from remote attacks on plant systems. While the deployment of the uni-directional barrier is critical to protection from external cyber threats, it also impacts remote access to plant data systems by authorized personnel. This elimination of remote access will require Licensees to develop and implement a detailed change management plan.

Another major activity is the performance of individual critical digital asset (CDA) assessments to identify individual asset security control remediation actions. Programs and procedures are being developed to implement the programmatic requirements of the regulation. The cyber security assessment teams are also being established for execution of program requirements. These teams are required to have extensive knowledge of plant systems and cyber security control technology. A comprehensive training program will be required to ensure competent personnel for program execution.

The following implementation schedule includes implementation milestones and the date when NextEra Energy Duane Arnold proposes to complete the implementation and enter the maintenance phase of the NRC approved Cyber Security Program. The established completion dates are contingent upon NRC approval of the Cyber Security Plan as submitted and upon NRC approval no later than June 30, 2011.

**NextEra Energy Duane Arnold**
**Cyber Security Plan Implementation Schedule**

| Implementation Milestone | Completion Date | Basis |
|---|---|---|
| Train and Qualify Cyber Security Assessment Team (CSAT)* | 11/15/2010 | The CSAT will require a broad and very specialized knowledge of information and digital systems technology. The CSAT will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team will require additional training in these areas to ensure adequate capabilities to meet the regulation requirements.<br><br>By the completion date, the following will be performed:<br>• Cyber security assessment procedures/tools will be developed and available;<br>• Qualifications for CSAT will be developed; and<br>• Training of the CSAT will be completed. |
| Develop Cyber Security Defensive Strategy (i.e., defensive model)* | 02/04/2011 | The Defensive Strategy expands upon the high level model in the Cyber Security Plan and requires assessment of existing site and corporate policies, comparison to new requirements, revisions as required, and communication to plant personnel.<br><br>By the completion date, the following will be performed:<br>• Documenting the defense-in-depth architecture and defensive strategy;<br>• Revisions to existing defensive strategy policies will be implemented and communicated; and<br>• Planning the implementation of the defense-in-depth architecture. |
| Identify Critical Systems (CSs) and Critical Digital Assets (CDAs)* | 6/15/2011 | By the completion date, the following will be performed:<br>• Critical Systems will be identified; and<br>• Critical Digital Assets will be identified. |
| Deployment of uni-directional communication barrier to ensure protection from remote attacks on plant systems* | 07/01/2012 | By the completion date, the following will be performed:<br>• The Defense in Depth Strategy will reflect implementation of the deterministic, one-way data diode technology.<br>• Engineering modifications required to configure, install and test the data diode devices will be completed. |
| Perform and document the cyber security | 03/01/2013 | Based on the existing cyber security program, it is known that the number of digital assets requiring assessment is extensive. As |

| Implementation Milestone | Completion Date | Basis |
|---|---|---|
| assessment described in the Cyber Security Plan* | | previously discussed, the CDA assessment methodology required for this regulation is extremely rigorous and deterministic. The completion of these assessments will require a significant commitment of resources. The assessments will not begin prior to having a fully established CSAT and the required procedures.<br><br>Performing the assessments will require participation of multiple disciplines and involve document reviews, system configuration evaluation, physical walk downs or electronic verification of every communication pathway for each CDA, and documentation of results. These tasks will need to be coordinated and scheduled to align with department resource availability and system access requirements.<br><br>By the completion date, the following will be performed:<br>• Cyber security assessments will be performed and documented. |
| Implement Cyber Security defense-in-depth architecture* | 06/01/2013 | The implementation of communication barriers protects the most critical SSEP functions from remote attacks on our plant systems. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers and other plant staff. This elimination of remote access to core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants.<br><br>Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled. Since software must be updated on and data retrieved from isolated systems, a method of patching, updating and scanning isolated devices will be developed. |
| Establish Cyber Security Program policies/procedures* | 07/01/2013 | The implementation of the cyber security program is expected to require policy/procedure development and/or upgrades for nearly every plant department. The procedural development for the cyber security program requirements and all of the individual |

| Implementation Milestone | Completion Date | Basis |
|---|---|---|
| | | security controls will be far-reaching. Many of the security controls will require development of the technical processes for implementing the control in a nuclear plant environment including development of new procedures for surveillances, and periodic monitoring and reviews. Procedure development will begin early in the implementation of the program and continue until the specified completion date.<br><br>By the completion date, the following will be performed:<br>• Policies/procedures will be updated to establish Cyber Security Program;<br>• The Cyber Security Assessment Procedure will be issued; and<br>• New policies/procedures or revision of existing policies/procedures in areas impacted by cyber security requirements will be developed and implemented. |
| Implement all modifications (outage and non-outage) and enter maintenance phase of NRC approved Cyber Security Program | 12/31/2014 | The date when NextEra Energy Duane Arnold proposes to complete the implementation and enter the maintenance phase of the NRC approved Cyber Security Program.<br>• All required modifications implemented<br>• All required procedures updated<br>• All required training completed |

*These milestones are considered commitments. Any commitment changes will be managed in accordance with NEI 99-04, “Guidelines for Managing NRC Commitment Changes.”