Entergy Nuclear Northeast
Indian Point Energy Center
450 Broadway, GSB
P.O. Box 249
Buchanan, NY 10511-0249
Tel 914 254 6700

Anthony J. Vitale
Site Vice President

April 28, 2017

NL-17-049

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
11555 Rockville Pike, OWFN-2 F1
Rockville, MD 20852-2738

SUBJECT: License Amendment Request – Cyber Security Plan Implementation Schedule
Indian Point Unit Nos. 1, 2, and 3
Docket Nos. 50-003, 50-247 and 50-286
License Nos. DPR-5, DPR-26 and DPR-64

REFERENCES:

1. NRC letter to Entergy, "Indian Point Nuclear Generating Unit Nos. 1, 2 and 3 - Issuance of Amendments Re: License Amendment Request - Cyber Security Plan (TAC Nos ME4212, ME4213, and ME4214)," dated August 2, 2011 (ML11152A027)

2. NRC letter to Entergy, "Issuance of Amendments Re: Cyber Security Plan Implementation Schedule Milestones," dated November 28, 2012 (ML12258A268)

3. NRC Internal Memorandum to Barry Westreich from Russell Felts, "Review Criteria for 10 CFR 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ML13295A467)

4. NRC letter to Entergy, "Issuance of Amendments - Cyber Security Plan Implementation Schedule," dated December 11, 2014 (ML14316A526)

5. NRC letter to Entergy, "Indian Point Nuclear Generating Unit Nos. 1, 2 and 3 – Issuance of Amendments Re: Cyber Security Plan Implementation Schedule," dated April 12, 2016 (ML16064A215)

6. Entergy letter NL-17-021 to NRC, "Notification of Permanent Cessation of Power Operations," dated February 8, 2017 (ML17044A004)

S001A
NMSS01
NRR
NMSS

Dear Sir or Madam:

Pursuant to 10 CFR 50.4, *Written communications*, and 10 CFR 50.90, *Application for amendment of license, construction permit, or early site permit*, Entergy Nuclear Operations, Inc. (Entergy) hereby requests a License Amendment for Indian Point Unit No. 1 (IP1), Operating License (OL) DPR-5, Docket No. 50-003, for Indian Point Unit No. 2 (IP2), OL DPR-26, Docket No. 50-247, and for Indian Point Unit No. 3 (IP3), OL DPR-64, Docket No. 50-286. In accordance with the guidelines provided by Reference 3, this request proposes a change to the Indian Point Energy Center (IPEC) Cyber Security Plan (CSP) Milestone 8 full implementation date as set forth in the CSP Implementation Schedule approved by Reference 1 and as amended by References 2, 4 and 5.

In Reference 6, Entergy notified the Nuclear Regulatory Commission (NRC) that power operations will permanently cease by April 30, 2020 at IP2 and by April 30, 2021 at IP3. In light of this, Entergy is requesting a change to the Milestone 8 date that is beyond the cessation of power operations dates, and beyond when the fuel is expected to have decayed to the point where the risk of a fire in the zirconium fuel cladding following a beyond-design-basis event involving the loss of spent fuel pool water inventory is significantly reduced, which is based on industry direction of 16 to 18 months.

Entergy is aware that other utilities are in a similar situation as IPEC, which is the premature shutdown of the facility. Entergy also understands that those utilities have also approached, or are going to approach, the NRC to eliminate the need to address Milestone 8 activities for their facilities. The circumstances at IPEC are slightly different, whereas, IPEC will have an operating plant for a longer period of time than those other facilities. As such, Entergy believes that additional actions over-and-above what the other utilities are requesting for Milestone 8 are warranted.

Therefore, by December 31, 2017, Entergy plans to implement a graded approach to full implementation of the CSP. The actions to be taken are as follows:

- Maintain Milestones 1 through 7 actions
- Implement the Entergy Fleet Milestone 8 Programs (Incident Response, Supply Chain, Training)
- Completion of Milestone 8 Assessments and Remediation for:
  - Security Systems
  - High Risk Safety Related Critical Digital Assets (CDAs) (such as Steam Generator level indication, Steam Generator Blowdown radiation monitors)
  - Balance of Plant (non-safety related)CDAs that can cause a direct turbine trip which results in a reactor trip (IP3 AMSAC)

Attachment 1 provides an analysis of the proposed changes, which have been evaluated in accordance with 10 CFR 50.91(a)(1), *Notice for public comment,* using criteria in 10 CFR 50.92(c), *Issuance of amendment.* Entergy has determined that the changes involve no significant hazards consideration. The bases for these determinations are included in Attachment 1. The proposed License Amendment requires no revised operating license pages (other than the Amendment No.) because of the current wording: "The ENO CSP was

approved by License Amendment No. [55, 266, and 243 for IP1, IP2 and IP3, respectively] and supplemental Amendments." However the License Amendment is required because the NRC SER, Reference 1, stated that "All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90." Attachment 2 contains a proposed revised CSP implementation schedule date for the full implementation of Milestone 8. Attachment 3 contains one revised commitment and one new commitment related to the full implementation of the IPEC CSP.

Entergy requests approval of the proposed license amendment by December 15, 2017. Once approved, the amendment will be effective as of the date of issuance and shall be implemented within 30 days. In accordance with 10 CFR 50.91(b), *State consultation*, a copy of this request and the associated Attachments is being submitted to the designated New York State official.

Should you have any questions concerning this letter or require additional information, please contact Mr. Robert Walpole, Manager, Regulatory Assurance at (914) 254-6710.

I declare under penalty of perjury that the foregoing is true and correct. Executed on April 28, 2017

Sincerely,

AJV/gd

Attachments:
1. Analysis of Proposed Operating License Change
2. Revised Cyber Security Plan Implementation Schedule
3. List of Regulatory Commitments

cc: Mr. Richard Guzman, Senior Project Manager, NRC NRR DORL
Ms. Kimberly A. Conway, Project Manager, NRC FSME DWMEP DURLD
Mr. Daniel H. Dorman, Regional Administrator, NRC Region 1
NRC Resident Inspector's Office
Mr. John B. Rhodes, President and CEO, NYSERDA
Ms. Bridget Frymire, New York State Dept. of Public Service

ATTACHMENT 1 TO NL-17-049

ANALYSIS OF PROPOSED OPERATING LICENSE CHANGE

ENTERGY NUCLEAR OPERATIONS, INC.
INDIAN POINT NUCLEAR GENERATING UNIT NOs. 1, 2 and 3
DOCKET NOs. 50-003, 50-247, and 50-286

1.0 SUMMARY DESCRIPTION

This license amendment request (LAR) includes a proposed change to the Indian Point Energy Center (IPEC) Cyber Security Plan (CSP) Implementation Schedule Milestone 8 full implementation date, and a proposed revision to the existing Operating License (OL) Physical Protection license condition for each unit. These changes are requested to support IPEC's transition from operating power plants to decommissioned power plants.

2.0 DETAILED DESCRIPTION

In Reference 1, the Nuclear Regulatory Commission (NRC) issued a license amendment to the Operating Licenses (OLs) for Indian Point Unit No. 1 (IP1), Indian Point Unit No. 2 (IP2), and Indian Point Unit No. 3 (IP3) that approved the IPEC CSP and associated implementation schedule for Milestones 1 through 8. The CSP Implementation Schedule approved by Reference 1 was utilized as a portion of the basis for the NRC's safety evaluation report provided in Reference 1. In Reference 8, the NRC issued a license amendment that revised the Milestone 8 full implementation date to December 31, 2017. In Reference 6, Entergy notified the NRC that IP2 and IP3 will cease power operations no later than April 30, 2020 and April 30, 2021, respectively. Since this notification, Entergy has continued to maintain the previously implemented cyber security Milestones 1 through 7, which were inspected for compliance by the NRC as described in References 5 and 7. In Reference 3, the NRC provided criteria to be used for evaluation of license amendment requests to revise the CSP Implementation Schedule Milestone 8 date. The information requested by Reference 3 is discussed in Section 3.0 below. In light of the cessation of all power operations by April 30, 2021, Entergy is proposing a change to the Milestone 8 full implementation date from December 31, 2017 to December 31, 2022.

Entergy will implement a graded approach to full implementation of the CSP. These actions are as follows:

- Maintain Milestones 1 through 7 actions
- Implement the Entergy Fleet Milestone 8 Programs, which include:
    - Incident Response – The process for identification, containment, eradication, recovery, and contingency planning related to a suspected or confirmed cyber event or attack involving one or more Critical Digital Assets (CDAs)
    - Supply Chain
    - Training – Three levels of Cyber Security training based upon the employee's job function(s): Awareness Training, Technical Training, Specialized Training
- Completion of Milestone 8 Assessments and Remediation for:
    - Security Systems
    - High Risk Safety Related Critical Digital Assets (CDAs). Items that fall into this category include CDAs such as:
        - Steam Generator level indication
        - Steam Generator Blowdown radiation monitors

Following is the approach used to identify High Risk Safety Related CDAs:

First, the total population of CDAs was separated into safety related and non-safety related components. The non-safety related CDAs were screened out. The remaining safety related CDAs were then screened using the Probabilistic Risk Assessment (PRA) models with the criteria discussed below to determine the High Risk Safety Related CDAs:

- Risk Achievement Worth (RAW) $\geq$ 2
- Risk Reduction Worth (RRW) $\geq$ 1.005

In determining the High Risk Safety Related CDAs, the first step was to look at the CDA list to determine which components were explicitly modeled in the PRA and, if so, to compare their risk importance measures to the above criteria used to determine risk significance for the Maintenance Rule [50.65 (a)(4)]. This comparison was performed in terms of both Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). CDAs were screened in at the component level if they satisfied the above criteria for risk significance for either CDF or LERF. There were no safety related CDAs that met the risk significance criteria, as there were no instruments that were explicitly modeled in the PRA. However, some CDAs were implicitly credited in the PRA either as part of the diagnosis of an event or procedural implementation of the required implementation of risk significant operator actions. For example, early isolation of a ruptured steam generator to prevent overfill is an important operator action in terms of LERF. High condenser air ejector radiation and high steam generator blowdown radiation (as indicated by recorders R-45 and R-49, respectively) are proceduralized indications used by the operator to diagnose a steam generator tube rupture. Therefore, recorders R-45 and R-49 were screened in, which is considered conservative given that other indications of a tube rupture are high main steamline radiation and increasing steam generator water level. .

A second screening was then performed based on system importance, with the rationale being that the components in the CDA list may not be risk significant individually but could be risk significant if the entire function or all the redundant components were unavailable. Systems are considered important if they have a RAW $\geq$ 20 (i.e., 10 times the component-level criteria for risk significance) or Fussell-Vesely (FV) importance $\geq$ 0.05 (5%). However, in many cases, even though a component may belong to an importance system doesn't mean it provides an important function. Nevertheless, some CDAs were conservatively screened in anyway. For example, Steam Generator (SG) level indication (which is related to AFW importance) is an important function. However, the CDAs associated with AFW are SG level recorders. In terms of risk, the recordersare not importantbecause they do not provide input into system actuation, nor are they needed to verify SG level. Nonetheless, these were conservatively screened in.

A final qualitative screening was performed to identify any CDAs that may be used by control room operators to respond to or mitigate an accident. For example, as previously discussed, SG blowdown radiation monitor recorder R-

49 provides one of the indications of a SG tube rupture. Therefore, the radiation monitors were conservatively screened in even though there are other indications available to help the operator diagnose a SG tube rupture.

Lastly, licensed operator input was obtained to ensure that additional components should not be screened in (i.e., that components relied upon to mitigate an accident were not inadvertently excluded). This review resulted in the identification of an additional number of High Risk Safety Related CDAs.

- Balance of Plant (non-safety related) CDAs that can cause a direct turbine trip which results in a reactor trip:
  - IP3 AMSAC

3.0 TECHNICAL EVALUATION

In November 2009, in accordance with 10 CFR 73.54, *Protection of digital computer and communications systems and networks*, (nuclear cyber security rule), Entergy submitted a proposed schedule for IPEC for achieving full compliance with the cyber security rule. The schedule was approved (Reference 1) and consists of eight milestones, with interim Milestones 1 through 7, as amended by Reference 2, being completed by December 31, 2012, and Milestone 8 (full compliance) to be completed by December 15, 2014. During the process of accomplishing Interim Milestones 1 through 7 and commencing Milestone 8 work, it became evident to Entergy that additional time would be required, and a schedule extension request for Milestone 8 to June 30, 2016, was approved by Reference 4. An additional extension for the Milestone 8 date to December 15, 2017 was approved by Reference 6. Milestones 1 through 7 were inspected for compliance in References 5 and 7. Presently, Milestone 8 (full compliance with the rule) is required to be completed by December 31, 2017. However, as described in Reference 8, Entergy intends to permanently cease power operations at IP2 and IP3 no later than April 30, 2020 and April 30, 2021, respectively. In support of this, a schedule extension request to December 31, 2022 for Milestone 8 full implementation is being requested.

Below is Entergy's discussion of the eight evaluation criteria provided in Reference 3.

1. **Identification of the specific requirement or requirements of the CSP that the licensee needs additional time to implement**

   Entergy requests that full implementation of CSP requirements per Milestone 8 be rescheduled from December 31, 2017 to December 31, 2022. The specific requirement is described in Cyber Security Plan, Section 3.1, "Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls."

   During this additional period Entergy will continue to comply with the requirements of Milestones 1 through 7. Also, as described in criterion 4 below, several elements of Milestone 8 will be completed.

2. Detailed justification that describes the reason additional time is required to implement the specific requirement or requirements identified

On February 8, 2017, in accordance with 10 CFR 50.82, *Termination of license*, Entergy notified the NRC of the intent to permanently cease power operations at IP2 and IP3 no later than April 30, 2020 and April 30, 2021, respectively. As identified in criterion 4 below, Entergy will be making a partial implementation of Milestone 8. Completion of the remaining Milestone 8 actions by December 31, 2017 is not a prudent use of Entergy resources because the CDAs that remain after partial implementation of Milestone 8 do not pose as significant a risk as the CDAs that are included in the partial implementation of Milestone 8. These CDAs involve remaining SSEP functions that will not be required after the reactor is certified to be permanently shut down and defueled. Therefore, the CDAs associated with those functions will no longer be required within a short time from now, and, will not be required to be protected subject to 10 CFR 73.54 after the 10 CFR 50.82 certifications have been submitted. As such, extending the remaining Milestone 8 actions until December 31, 2022 has no adverse effect on nuclear safety given that Entergy is required to maintain the previously implemented actions for Milestones 1 through 7, and is partially implementing actions for Milestone 8.

3. Proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available

The proposed completion date for Milestone 8 is December 31, 2022. By this date, the IPEC operating reactors will have ceased power operations, and it is anticipated that the reactors will have been defueled, and the fuel stored in the spent fuel pools are expected to have decayed to the point where the risk of a fire in the zirconium fuel cladding following a beyond-design-basis event involving the loss of spent fuel pool water inventory is significantly reduced, which is based on industry direction of 16 to 18 months. Once these plant conditions are achieved, the CSP license conditions are no longer required and Entergy plans to submit a LAR to remove the conditions from the OLs of the IPEC units.

4. Evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the overall cyber security program in the context of milestones already completed

The impact of the requested additional implementation time on the effectiveness of the overall cyber security program is considered to be very low, because the Interim Milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against threat vectors associated with external connectivity (both wired and wireless), and portable digital media and devices. Additionally, extensive physical and administrative measures are already in place for CDAs pursuant to the IPEC Security Plan and Technical Specification requirements. In the context of cyber security milestones already completed, the following is noted:

a. An Entergy Cyber Security Assessment Team (CSAT) has been implemented consisting of highly experienced personnel knowledgeable in reactor and balance-of-plant design, licensing, safety, security, emergency preparedness, information technology, and cyber security. The CSAT is provided with the authority, via written procedure, to perform the analyses and oversight activities described in the CSP.

b. Critical systems and CDAs have been identified, documented, and entered in a controlled database.
c. The plant process computer network and the plant security computer network have been deterministically isolated per the requirements of cyber security Interim Milestone 3.
d. Safety-related, important-to-safety, and security CDAs have been extensively reviewed and verified (or modified) to be deterministically isolated and not to employ wireless network technology.
e. Procedures have been implemented for portable digital media and devices periodically connected to CDAs, per NEI 08-09, Revision 6, Appendix D, Section 1.19.
f. CDAs associated with physical security target sets have been analyzed per the requirements of the CSP Section 3.1.6 and either (1) verified to satisfy the Technical Cyber Security Controls described in NEI 08-09, Revision 6, Appendix D or (2) actions required to satisfy the Technical Cyber Security Controls described in NEI 08-09, Revision 6, Appendix D, are captured in the Corrective Action Program (CAP).
g. Employees have been provided with training on cyber security awareness, tampering, and control of portable digital media and devices periodically connected to CDAs.

Additionally, although not required until Milestone 8, the following elements of the Cyber Security Program will be completed:

- Maintain Milestones 1 through 7 actions
- Implement the Entergy Fleet Milestone 8 Programs (Incident Response, Supply Chain, Training)
- Completion of Milestone 8 Assessments and Remediation for:
  - Security Systems
  - High Risk Safety Related CDAs (such as Steam Generator level indication, Steam Generator Blowdown radiation monitors)
  - Balance of Plant (non-safety related) CDAs that can cause a direct turbine trip which results in a reactor trip (IP3 AMSAC)

5. Description of the methodology for prioritizing completion of work for CDAs associated with significant SSEP consequences and with reactivity effects in the balance of plant

CDAs are plant components that are subject to the maintenance prioritization and normal work management process which places the highest priority on apparent conditions adverse to quality in system, structure, and component (SSC) design function and related factors such as safety risk and nuclear defense-in-depth, as well as threats to continuity of electric power generation in the balance-of-plant (BOP). Further, in regard to deterministic isolation and control of portable media and mobile devices (PMMDs) for safety-related, important-to-safety (including BOP), and security CDAs, maintenance of one-way or air-gapped configurations and implementation of control of PMMDs remains high priority. This prioritization enabled timely completion of cyber security Interim Milestones 3 and 4.

Entergy continues to give prompt attention to any emergent issues with CDAs that would potentially challenge the established cyber protective barriers.

6. **Discussion of the cyber security program performance up to the date of the license amendment request**

No compromise of SSEP function by cyber means has been identified. As documented in Reference 5, an NRC inspection at IPEC of Entergy's compliance with Milestones 1 through 7 was concluded on October 2, 2015, and findings were designated as having very low safety significance (green non-cited, granted enforcement discretion). Additionally, a Problem Identification and Resolution Sample Inspection (Reference 7) was concluded on March 2, 2017 and the one finding was designated as having very low safety significance (green non-cited). Further, an annual Entergy quality assurance (QA) audit has been conducted every year since 2013 pursuant to the physical security program review required by 10 CFR 73.55(m), *Security program reviews*. The QA audit includes review of cyber security program implementation, and there have been no significant audit findings related to overall cyber security program performance and effectiveness during these audits. In preparation for the NRC inspection, a Milestone 1-7 self-assessment was performed in June 2015. In addition, a self-assessment was performed in January 2017 prior to an NRC Problem Identification & Resolution (PI&R) Sample Inspection. All the deficiencies from both self-assessments were self-identified, entered into the corrective action program and resolved in a timely manner.

7. **Discussion of cyber security issues pending in the CAP**

No cyber security issues that would constitute a threat to proper CDA function or that would call into question cyber security program effectiveness are currently pending in the corrective action program. Currently there is one Condition Report (CR) in the Corrective Action Program from the PI&R Sample Inspection (Reference 7) that was concluded on March 2, 2017. It involves the assessment methodology to meet the NEI 08-09 App D controls for the assessments of CDS CDAs that were reviewed. The subject CDAs have been reassessed and two remaining corrective actions involve reviews of the reassessed CDAs and of initial CDA assessments by qualified IPEC personnel to ensure and validate assessment quality. Two other CRs are considered administrative in nature - one documents the missed synchronization of the safety related field of the component database and the CDA database; one documents the need to reclassify components as CDAs, which have been added to the CDA database and which are in the process of being added to the component database.

8. **Discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications**

Modifications completed include those required to deterministically isolate Level 3 and 4 CDAs, as required by nuclear cyber security implementation schedule interim Milestone 3. A modification not yet implemented installs the hardware components to remediate and reduce the susceptibility of cyber assets to cyber-attack over a range of attack tactics, techniques, and procedures to comply with the Cyber Security Program. This modification installs infrastructure upgrades to the plant's security systems. The required upgrades to be implemented are Security Intrusion and Event Monitoring (SIEM), Intrusion Detection

System, Antivirus, and various other software security solutions. This entails upgrades to the Level 4 Security System network to assure the infrastructure is compliant with the Cyber Security Requirements of NEI-08-09 Milestone 8 Appendix D and E. This modification will also include installing physical security to protect certain critical digital assets.

This LAR includes no specific proposed changes to the existing operating licenses for IP1, IP2, and IP3, respectively as discussed in Section 4.1. This LAR contains the proposed Revised CSP Implementation Schedule (Attachment 2) and provides a revised list of regulatory commitments (Attachment 3).

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

10 CFR 73.54, *Protection of digital computer and communications systems and networks*, requires licensees to maintain and implement a CSP. The OLs of IP1, IP2, and IP3, DPR-5, DPR-26, and DPR-64, respectively, include a Physical Protection license condition as follows: "ENO shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The ENO CSP was approved by License Amendment No. [55, 266, and 243 for IP1, IP2 and IP3, respectively] and supplemental amendments." The NRC approval of this license condition (Reference 1) stated that "All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90." This License Amendment requests a change to the Implementation Milestone 8 completion date in the CSP.

4.2 Significant Safety Hazards Consideration

Entergy is requesting an amendment to the IP1, IP2 and IP3 Facility Operating Licenses to revise Milestone 8 required by the Physical Protection license condition as it relates to the CSP. This change requires an Amendment to the IP1, IP2 and IP3 Facility Operating Licenses to allow the proposed deviation. Specifically, Entergy is proposing a change to the Implementation Milestone 8 completion date.

Entergy 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 change involve a significant increase in the probability or consequences of an accident previously evaluated?

   Response: No.

   The proposed change to the CSP Implementation Schedule does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components relied upon to mitigate the

consequences of postulated accidents and has no impact on the probability or consequences of an accident previously evaluated.

Therefore, the proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

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

Response: No.

The proposed change to the CSP Implementation Schedule does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components relied upon to mitigate the consequences of postulated accidents and does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

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

Response: No.

Plant safety margins are established through limiting conditions for operation, limiting safety system settings, and safety limits specified in the technical specifications. The proposed change to the CSP Implementation Schedule does not involve these items. In addition, the milestone date delay for full implementation of the CSP has no substantive impact because other measures have been taken which provide adequate protection during this period of time. Because there is no change to established safety margins as a result of this change, the proposed change does not involve a significant reduction in a margin of safety.

Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Based on the above, Entergy 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 provides a change to the CSP Implementation Schedule. The proposed amendment meets the eligibility criterion for a categorical exclusion set forth in 10 CFR 51.22(c)(12). Therefore, pursuant to 10 CFR 51.22(b) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

6.0 REFERENCES

1. NRC letter to Entergy, "Indian Point Nuclear Generating Unit Nos. 1, 2 and 3 - Issuance of Amendments Re: License Amendment Request - Cyber Security Plan (TAC Nos ME4212, ME4213, and ME4214," dated August 2, 2011 (ML11152A027)

2. NRC letter to Entergy, "Indian Point Nuclear Generating Unit Nos. 1, 2 and 3 - Issuance of Amendments Re: Cyber Security Plan Implementation Schedule Milestones (TAC Nos. ME8885, ME8886, and ME8887)," dated November 28, 2012 (ML12258A268)

3. NRC Internal Memorandum to Barry Westreich from Russell Felts, "Review Criteria for 10 CFR 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ML13295A467)

4. NRC letter to Entergy, "Indian Point Nuclear Generating Unit Nos. 1, 2 and 3 - Issuance of Amendments Re: Cyber Security Plan Implementation Schedule (TAC Nos. MF3409 and MF3410)," dated December 11, 2014 (ML14316A526)

5. NRC letter to Entergy, "Indian Point Nuclear Generating Units 2 and 3 – Temporary Instruction 2201/004, Inspection of Interim Cyber Security Milestones 1-7, Reports 05000247/2015405 and 05000286/205405," dated October 21, 2015 (ML15295A050)

6. NRC letter to Entergy, "Indian Point Nuclear Generating Unit Nos. 1, 2 and 3 – Issuance of Amendments Re: Cyber Security Plan Implementation Schedule, (TAC Nos. MF6368, MF6369, and MF6370)," dated April 12, 2016 (ML16064A215)

7. NRC letter to Entergy, "Indian Point Nuclear Generating Units 2 and 3 – Problem Identification and Resolution Cyber Security Inspection Report 05000247/2017405 and 05000286/2017405," dated March 27, 2017 (ML17087A047)

8. Entergy letter NL-17-021 to NRC, "Notification of Permanent Cessation of Power Operations," dated February 8, 2017 (ML17044A004)

ATTACHMENT 2 TO NL-17-049

REVISED CYBER SECURITY PLAN
IMPLEMENTATION SCHEDULE

ENTERGY NUCLEAR OPERATIONS, INC.
INDIAN POINT NUCLEAR GENERATING UNIT NOs. 1, 2 and 3
DOCKET NOs. 50-003, 50-247, and 50-286

Revised Cyber Security Plan Implementation Schedule

#	Implementation Milestone	Completion Date	Basis
8	Full implementation of the IPEC Cyber Security Plan for all safety, security, and emergency preparedness (SSEP) functions will be achieved	December 31, 2022	By the completion date, the IPEC Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refueling outage for implementation.

ATTACHMENT 3 TO NL-17-049

LIST OF REGULATORY COMMITMENTS

ENTERGY NUCLEAR OPERATIONS, INC.
INDIAN POINT NUCLEAR GENERATING UNIT NOs. 1, 2 and 3
DOCKET NOs. 50-003, 50-247, and 50-286

List of Regulatory Commitments

The following table identifies those actions committed to by Entergy in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments.

COMMITMENT	TYPE (Check One)		SCHEDULED COMPLETION DATE (If Required)
	ONE-TIME ACTION	CONTINUING COMPLIANCE	

Partial implementation of Milestone 8
• Implement the Entergy Fleet Milestone 8 Programs
• Completion of Milestone 8 Assessments and Remediation for:
  ▪ Security Systems
  ▪ High Risk Safety Related CDAs
  ▪ Balance of Plant (non-safety related) CDAs that can cause a direct turbine trip which results in a reactor trip
	X		December 31, 2017

Full implementation of the IPEC Cyber Security Plan for all safety, security, and emergency preparedness functions will be achieved	X		December 31, 2022