Exelon Generation

10CFR 50.90

April 10, 2017

U.S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, D.C. 20555-0001

Oyster Creek Nuclear Generating Station
Renewed Facility Operating License No. DPR-16
USNRC Docket No. 50-219

Subject: License Amendment Request Regarding Revision to Cyber Security Plan Milestone 8 Completion Date

References:

1. NRC Letter to Exelon, "Oyster Creek Nuclear Generating Station – Issuance of Amendment Regarding the Exelon Cyber Security Plan," dated August 10, 2011 (ADAMS Accession No. ML111861341)

2. NRC Letter to Exelon, "Issuance of Amendments Revising the Completion Date for Milestone 8 of the Cyber Security Plan," dated July 30, 2015 (ADAMS Accession No. ML15153A282)

3. Memorandum from R. Felts, (U.S. Nuclear Regulatory Commission) to B. Westreich (U.S. Nuclear Regulatory Commission), "Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ADAMS Accession No. ML13295A467)

4. Exelon Letter to NRC, "Permanent Cessation of Operations at Oyster Creek Nuclear Generating Station," dated January 7, 2011 (ADAMS Accession No. ML110070507)

5. Exelon Letter to NRC, "License Amendment Request Regarding Revision to Cyber Security Plan Milestone 8 Completion Date," dated April 4, 2017

In accordance with the provisions of 10 CFR 50.90, Exelon Generation Company, LLC (Exelon), is submitting a request for an amendment to the Renewed Facility Operating License (RFOL) No. DPR-16 for Oyster Creek Nuclear Generating Station (OCNGS). This proposed amendment requests U.S. Nuclear Regulatory Commission (USNRC) approval of a change to the Cyber Security Plan (CSP) Milestone 8 completion date (hereinafter referred to as MS8), as set forth in the CSP Implementation Schedule as approved by the USNRC in Reference 1 and as modified in Reference 2.

In Reference 1, the NRC issued an amendment to the OCNGS RFOL which approved the Exelon CSP and implementation schedule. The approved schedule stated the date that full implementation of the Exelon CSP for all Safety-Related, Security and Emergency Preparedness (SSEP) functions (MS8) would be completed. In Reference 2, the NRC issued an amendment revising the completion date for MS8 of the Exelon CSP based on justifications provided to meet the guidance in Reference 3.

In Reference 4, Exelon notified the NRC of Exelon's plans to permanently cease operations at OCNGS, pursuant to 10 CFR 50.82(a)(1)(i). Exelon is requesting an extension to the Milestone 8 completion date of the Exelon CSP for the OCNGS.

Attachment 1 provides an evaluation of the requested extension request and amendment to the OCNGS RFOL that uses the guidance detailed in Reference 3. This amendment request includes the existing FOL marked up to show the proposed change (Attachment 2), the revised Cyber Security Commitment (Attachment 3), and the associated revised CSP Implementation Schedule (Attachment 4).

These proposed changes have been reviewed and approved by the OCNGS Plant Operations Review Committee in accordance with the requirements of the Exelon Quality Assurance Program.

In Reference 5, Exelon stated that Attachments 1, 3 and 4 were considered to contain security related information and requested these Attachments to be withheld in accordance with 10 CFR 2.390. The request was based on similar Exelon submittals and an industry template for the MS8 completion date extension requests for sites designated for Decommissioning. On April 5, 2017, the NRC determined that the information in Reference 5 does not contain security related information and requested a resubmittal without the request for withholding. This letter provides the requested resubmittal of Reference 5 including each of the Attachments. There are no changes to the Attachments contained in Reference 5 other than removal of the headers and footers regarding the request to withhold security related information.

Exelon requests approval of the proposed amendment by November 2, 2017. Once approved, the amendment will be implemented no later than December 31, 2017.

In accordance with 10 CFR 50.91, a copy of this amendment request, with attachments, is being provided to the designated State Official.

If you should have any questions or require additional information, please contact Mr. David Neff at 610-765-5631.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the 10th day of April 2017.

Respectfully,

D. A Helker

David P. Helker
Manager, Licensing & Regulatory Affairs
Exelon Generation Company, LLC

Attachment 1 - Evaluation of Proposed Change
Attachment 2 - Proposed Facility Operating License Changes (Mark-Up)
Attachment 3 - Revised Cyber Security Commitment
Attachment 4 - Revised Cyber Security Plan Implementation Schedule

cc: USNRC Region I, Regional Administrator
USNRC Project Manager, NRR - Oyster Creek Nuclear Generating Station
USNRC Senior Resident Inspector - Oyster Creek Nuclear Generating Station
Director, Bureau of Nuclear Engineering, New Jersey,
Dept. of Environmental Protection

ATTACHMENT 1

Revision to Cyber Security Plan Milestone 8 Completion Date

Evaluation of Proposed Changes

Oyster Creek Nuclear Generating Station

Renewed Facility Operating License No. DPR-16

1.0 SUMMARY DESCRIPTION

Exelon Generation Company, LLC (Exelon), is submitting a request for an amendment to the Renewed Facility Operating License (RFOL) No. DPR-16 for Oyster Creek Nuclear Generating Station (OCNGS). This amendment request proposes a change to the Implementation Milestone Regulatory Commitment for the Exelon Cyber Security Plan (CSP) Milestone 8 full implementation date (hereinafter referred to as the MS8 date) as set forth in the Exelon CSP Implementation Schedule. The current MS8 date of December 31, 2017, was approved by the U. S. Nuclear Regulatory Commission (USNRC) in Reference 6.2. Exelon proposes to extend the MS8 date from the current date of December 31, 2017, to August 31, 2021, when OCNGS will be permanently shutdown and fuel stored in the spent fuel pool (SFP) will have sufficiently decayed. Correspondingly, additional text is proposed that adds the RFOL amendment number related to this amendment request to the existing OCNGS Facility Operating License Condition that requires implementation of the CSP.

Attachment 2 contains the existing RFOL marked up to show the proposed change, Attachment 3 contains the revised Cyber Security Commitment, and Attachment 4 contains the associated revised CSP Implementation Schedule.

2.0 DETAILED DESCRIPTION

Cyber security requirements are codified in 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 10 CFR 73.1. 10 CFR 73.54 specifically requires operating licensees to implement a CSP that satisfies the requirements of the Rule in accordance with a USNRC-approved CSP implementation schedule.

On August 10, 2011, and July 30, 2015, the USNRC issued amendments to the OCNGS RFOL (References 6.1 and 6.2). The RFOL amendments incorporated the CSP and associated implementation schedule, and revised the RFOL to provide a license condition to require the licensees to fully implement and maintain in effect all provisions of the USNRC-approved CSP. Any change to the USNRC-approved CSP implementation schedule requires prior USNRC approval pursuant to 10 CFR 50.90. With issuance of RFOL Amendment 288 on July 30, 2015, the CSP MS8 completion date is currently December 31, 2017.

The physical, technical, operational and management Cyber Security controls associated with Milestones 1 through 7 (hereafter shown as MS1-7) of the CSP Implementation Schedule and the "Good Faith Letter" (Reference 6.4) required actions have been implemented for OCNGS. These Cyber Security controls continue to provide the intended high degree of protection against cyber-attacks and radiological sabotage.

In Reference 6.3, Exelon notified the NRC of Exelon's plans to permanently cease operations at OCNGS no later than December 31, 2019, pursuant to 10 CFR 50.82(a)(1)(i). Exelon is requesting an extension to the Milestone 8 completion date of the Exelon CSP for the OCNGS to no later than August 31, 2021. This date is based on the date when OCNGS will have permanently ceased operations (Reference 6.3) and additional time for Exelon to submit and for the NRC to process a separate request for an amendment to remove the Facility Operating License Condition that

requires implementation of the CSP. This separate request for an amendment will be submitted after OCNGS has permanently ceased operations. The August 31, 2021, extension date is technically based on meeting the spent fuel decay heat level evaluation criteria in NSIR/DPR-ISG-02, Emergency Planning Exemption Requests for Decommissioning Nuclear Power Plants. This criteria states that, in the event of a beyond design basis event resulting in the partial drain down of the SFP to the point that cooling is not effective, there is at least 10 hours (assuming an adiabatic heatup) from the time that the fuel is no longer being cooled until the hottest fuel assembly reaches 900 degrees Celsius. This amount of spent fuel decay prevents initiation of a zirconium fire, and resulting significant radiological release, in the event of a beyond-design-basis accident scenario that involves a major loss of inventory from the SFP. With a reactor shutdown by December 31, 2019, it is preliminarily estimated that this criteria would be met by June 30, 2021.

This license amendment request proposes to change the MS8 implementation date from December 31, 2017, to August 31, 2021. The technical justification to support the MS8 extension is provided in Section 3.0, below. The corresponding revision to the Cyber Security Commitment is provided in Attachment 3. The revision to the MS8 full implementation date in the CSP Implementation Schedule is provided in Attachment 4.

3.0 TECHNICAL EVALUATION

In an October 24, 2013, USNRC memorandum between the Director and Deputy Director Cyber Security Directorate from the Office of Nuclear Security and Incident Response (NSIR), the USNRC provided review criteria for licensee MS8 extension requests (Reference 6.5). Below is a response to each of the eight (8) review criteria provided in Reference 6.5 to support this extension request.

1) Identification of the specific requirement or requirements of the cyber security plan that the licensee requests additional time to implement.

Exelon requests that full implementation of the CSP requirements per MS8 be extended from December 31, 2017, to August 31, 2021. During this additional period the requirements of MS1-7 will be maintained.

2) Detailed justification that describes the reason the licensee requires additional time to implement the specific requirement or requirements identified.

Additional time is being requested to meet full compliance with MS8 for a plant designated to be permanently shutdown and defueled. On January 7, 2011, Exelon notified the USNRC of plans to permanently cease operations of OCNGS (Reference 6.3). Computations have estimated that by June 30, 2021, the decay heat for all spent nuclear fuel stored in the spent fuel pool should be decayed to a point where a loss of cooling cannot lead to zirconium hydride reactions and offsite releases. An additional two months is added to the extension request for Exelon to submit and for the NRC to process a separate request for an amendment to remove the Facility Operating License Condition that requires implementation of the CSP. The requested extension period will include 2 years of plant operations and 1 year and 8 months of shutdown conditions.

Implementation of cyber security protections provided by completed actions for MS1-7 of the CSP has been completed, verified and inspected. These substantial protections provide for reduced risk to the public from a Design Basis Accident (DBA) or Design Basis Threat (DBT) from a potential cyber-attack. Since initial implementation in December 2012, and as assessed by the USNRC, the cyber security protections provided by completed actions for MS1-7 have provided sufficient cyber security controls for over four years to mitigate the threat/attack pathways at OCNGS. OCNGS has no Critical Digital Assets (CDAs) in any of the target sets, thereby further limiting the risk of radiological consequences from a potential cyber-security attack. The cyber security controls implemented for MS1-7 will be maintained during the short extension period providing the same level of protection for the threat/attack pathways.

Activities to complete CDA assessments and implementation of additional cyber security controls by the current MS8 commitment date would increase the complexity of the plant equipment with little or no increase in protection of the Safety Related, Security and Emergency Preparedness (SSEP) functions supported by the existing Critical Systems (CSs) and CDAs. Decommissioning activities, to start after December 31, 2019, will be focused on efforts to reduce plant equipment that will further reduce plant risk and potential consequences of a cyber-attack.

Exelon has determined that the existing cyber security controls will provide a high degree of protection for the threat/attack vectors and protection against cyber-attacks and radiological sabotage during the short time period of the MS8 extension.

3) A 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 MS8 is August 31, 2021.

4) An evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the licensee's overall cyber security program in the context of milestones already completed.

Based on the CSP Implementation Plan activities completed under MS1-7, the "Good Faith Letter" (Reference 6.4) required actions and the continued maintenance of these actions, the OCNGS Cyber Security defensive posture and cyber security program will continue to be effective in significantly mitigating the risk of the DBT via cyber means. Exelon will continue to ensure that digital computer and communication systems and networks are adequately protected against cyber-attacks.

OCNGS has completed the implementation of the MS1-7 and the "Good Faith Letter" (Reference 6.4) required actions. The completed activities include:

A. Completion of Milestone 1 established the Cyber Security Assessment Team (CSAT) as described in CSP Section 3.1.2, "Cyber Security Assessment Team." The CSAT will remain in place with the required broad knowledge. Extending the due date of MS8 will not affect the CSAT.

B. Completion of Milestone 2 identified CSs and CDAs as described in CSP Section 3.1.3, "Identification of Critical Digital Assets." Extending the due date for MS8 will not affect the work completed for Milestone 2. The process of identifying CS and CDAs has been incorporated into Station Procedures. Future design changes will be processed in accordance with the existing Station Procedures that will ensure that CSs and CDAs are appropriately identified and the list of CSs and CDAs is maintained current.

C. Completion of Milestone 3 installed a deterministic one-way device (i.e., data diode) between lower level devices (i.e., Levels 0, 1, and 2) and the higher level devices (i.e., Levels 3 and 4) as described in CSP Section 4.3, "Defense-in-Depth Protective Strategies." Extending the due date for MS8 will not affect the work completed for Milestone 3. Future design changes will be processed in accordance with the existing Station Procedures that will ensure continued protection of CDAs provided by the cyber security defensive levels including preventing data diode bypasses.

D. Completion of Milestone 4 implemented security controls as described in NEI 08-09, Revision 6, Appendix D 1.19, "Access Control for Portable and Mobile Devices." Extending the due date for MS8 will not affect the controls presently applied to portable and mobile devices for Milestone 4. Continued implementation of existing Station Procedures will ensure continued application of these cyber security controls.

E. Completion of Milestone 5 implemented guidance for observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in NEI 08-09, Revision 6, Appendix E, Section 4.3, "Personnel Performing Maintenance and Testing Activities." Extending the due date for MS8 will not affect the insider mitigation program. Station Procedures have been implemented to ensure continued application of these cyber security controls.

F. Completion of Milestone 6 identified, documented, and implemented technical cyber security controls as described in NEI 08-09, Revision 6, Appendix D, and CSP Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls." OCNGS has no CDAs in any of the target sets. Extending the due date for MS8 will not affect the evaluations performed or controls established to date. Station Procedures are in place to periodically evaluate the target set population.

G. Completion of Milestone 7 required implementation of ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented as described in CSP Section 4.4, "Ongoing Monitoring and Assessment." OCNGS has no CDAs in any of the target sets. Extending the due date for MS8 will not affect the controls established to date. Station Procedures are in place to periodically evaluate the target set population. Monitoring and assessment of the continued implementation of the MS1-7 commitments will be performed commensurate with the number of CDAs that remain.

The MS8 implementation date extension has no effect on the overall effectiveness of the OCNGS Cyber Security Program in the context of the Milestones already completed. Assessment of the continued implementation of the MS1-7 commitments will be performed in accordance with existing Station Procedures commensurate with the number and SSEP

function of the CSs and CDAs to ensure the level of cyber security protection is maintained during the extension period. This will include an ongoing review of industry issues and initiatives to identify necessary improvements in the cyber security program.

OCNGS has implemented additional onsite security measures related to the Reactor Building Vital Areas (Reference 6.6) that also provides augmented physical protections for CSs and CDAs. The five (5) specific enhanced security measures implemented under this RFOL amendment include the following:

1. Controls for limiting physical access to the reactor building,
2. Train general personnel of site security awareness,
3. Increase operations, security, security supervisors, and radiation protection personnel tours of the plant,
4. Increase security focus awareness training for Operations, Security, Security Supervisors, and Radiation Protection personnel, and
5. Revise security-related procedures to implement the alternative measures.

No cyber security incidents have been identified since completion of MS1-7 in 2013 at OCNGS. A program is in place where potential threats based on component vulnerabilities are regularly screened for potential fleet and site vulnerability evaluations. One potential vulnerability has been identified and a modification will implement a software patch for a security computer. There are no other known issues requiring remediating action at OCNGS.

Once OCNGS is permanently shutdown and defueled, the reduction in the number of digital computers and communication systems and networks reduces the number of attack pathways for a cyber-attack during the decommissioning period.

Exelon has concluded that the MS8 completion date extension will have a negligible impact on the effectiveness of the overall cyber security program.

5) A description of the licensee's methodology for prioritizing completion of work for critical digital assets associated with significant safety, security, or emergency preparedness consequences and with reactivity effects in the balance of plant.

The Exelon methodology for prioritizing protection of CSs and CDAs is focused on maintaining the existing cyber security protections provided by the MS1-7 commitments, on continued safe plant operations and, once shutdown, on reducing plant equipment that will further reduce plant risk and consequences of a potential cyber-attack. Most notably, safety-related, important-to-safety, and security CSs and CDAs will continue to be deterministically isolated from external networks; stringent control of portable media and mobile devices connected to CDAs will continue, including use of stand-alone scanning kiosks, and implementation of technical cyber security controls and security officer observation for CDAs that support physical security target set functions (if a target set CDA is identified in the future). Additionally, OCNGS has implemented and will maintain the Exelon fleet procedures governing CDA configuration management, cyber security incident response and recovery, cyber security training, identification of rogue connections, and CDA physical protections.

Activities to complete CDA assessments and implementation of additional cyber security controls by the current MS8 commitment date would increase the complexity of the plant equipment with little or no increase in protection of the SSEP functions supported by the existing CSs and CDAs. Decommissioning activities, to start after December 31, 2019, will be focused on efforts to reduce plant equipment that will further reduce plant risk and potential consequences of a cyber-attack.

6) A discussion of the licensee's cyber security program performance up to the date of the license amendment request.

Exelon uses the Corrective Action Program (CAP) to document all cyber security issues in order to trend, correct, and improve the Exelon cyber security program. The CAP documents and tracks, from initiation through closure, all cyber security required actions including issues identified during on-going program assessment activities. Adverse trends are monitored for cyber security program improvement and addressed in the CAP.

A Nuclear Oversight audit of CSP MS1-7 conducted in December 2016 and on-going Quality Assurance surveillances under the physical security surveillance program have concluded that OCNGS has an effective cyber security program. Any audit issues identified were entered into the CAP and addressed for cyber security program improvement.

An OCNGS self-assessment for MS1-7 conducted in June 2014 concluded that OCNGS has an effective CSP. Issues identified during the self-assessments were entered into the CAP and addressed for cyber security program improvement.

Additionally, on-going monitoring and time-based periodic actions provide continuing program performance monitoring.

On August 15, 2014, the NRC completed a cyber-security inspection at OCNGS for Cyber Security MS1-7, which resulted in no NRC findings and two licensee identified findings of very low significance (Reference 6.7). The two identified findings have been remediated.

7) A discussion of cyber security issues pending in the licensee's corrective action program.

There are no cyber security related issues that would constitute a threat to proper CDA function or that would call into question cyber security program effectiveness that are currently pending in the CAP. There is one open cyber security related modification pending at OCNGS pertaining to installation of a software patch for a security computer that is expected to be implemented by December 31, 2017.

8) A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

The following modifications have been implemented at OCNGS.

- Data Diodes segregating Level 3 from Level 2 have been implemented at OCNGS.

- Isolated portable media scanning kiosk stations have been deployed at OCNGS. These devices or an equivalent technology will be maintained current with the latest malware detection signatures consistent with the Exelon fleet procedures.

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

The USNRC issued Amendment 288 (Reference 6.1) to the Oyster Creek Nuclear Generating Station (OCNGS) Renewed Facility Operating License (RFOL) No. DPR-16. The RFOL Amendment approved a revised completion date for the Cyber Security Plan implementation schedule for Milestone 8 and added the associated RFOL Amendment number 288 to the existing cyber security License Condition. Any change to the USNRC-approved Cyber Security Plan (CSP) implementation schedule requires prior USNRC approval pursuant to 10 CFR 50.90. The USNRC issued review criteria for Cyber Security Implementation Schedule Milestone 8 License Amendment requests (Reference 6.5).

4.2 Precedent

The NRC has previously issued amendments for MS8 completion date extensions for licensees that have provided the responses to the criteria in Reference 6.5. This request utilizes the same approach as previous requests.

4.3 No Significant Hazards Consideration

Exelon Generation Company, LLC (Exelon) 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 amendment request proposes a change to the Oyster Creek Nuclear Generating Station (OCNGS) Cyber Security Plan (CSP) Milestone 8 (MS8) completion date as set forth in the CSP Implementation Schedule and associated regulatory commitments. The revision of the MS8 completion date for the CSP does not involve modifications to any safety-related structures, systems, or components (SSCs). The revision of the CSP Implementation Schedule will not alter previously evaluated design basis accident analysis assumptions, add any accident initiators, modify the function of the plant safety-related SSCs, or affect how any plant safety-related SSCs are operated, maintained, modified, tested, or inspected.

   Therefore, the proposed change 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 amendment request proposes a change to the CSP MS8 completion date as set forth in the CSP Implementation Schedule and associated regulatory commitments. The revision of the MS8 completion date for the CSP does not involve modifications to any safety-related SSCs. No new accident scenarios, failure mechanisms, or limiting single failures are introduced as a result of this proposed amendment.

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

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

   Response: No

   The amendment request proposes a change to the CSP MS8 completion date as set forth in the CSP Implementation Schedule and associated regulatory commitments. The revision of the MS8 completion date for the CSP does not involve modifications to any safety-related SSCs. The proposed amendment has no effect on the structural integrity of the fuel cladding, reactor coolant pressure boundary, or containment structure.

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

Based on the above, Exelon concludes that the proposed amendment does not involve a 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.

4.4 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 is confined to safeguards matters, organizational and procedural matters; and administrative changes; and does not involve any significant construction impacts. Accordingly, the proposed amendment meets the eligibility criterion for 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 proposed amendment.

6.0 REFERENCES

6.1. Letter from J. S. Wiebe, (U.S. Nuclear Regulatory Commission) to M. J. Pacilio, (Exelon), "Issuance of Amendments Regarding the Exelon Cyber Security Plan," dated August 10, 2011.

6.2. Letter from B. Purnell (USNRC) to B. C. Hanson, (Exelon), "Issuance of Amendments Revising the Completion Date for Milestone 8 of the Cyber Security Plan," dated July 30, 2015.

6.3. Letter from K. R. Jury, (Exelon) to U.S. Nuclear Regulatory Commission, "Permanent Cessation of Operations at Oyster Creek Nuclear Generating Station," dated January 7, 2011 (ADAMS Accession No. ML110070507).

6.4. Memorandum from B. C. Westreich (USNRC) to C. G. Miller (USNRC), et. al., "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for 'Good- Faith' Attempt Discretion," dated July 1, 2013.

6.5. Memorandum from R. Felts, (USNRC) to B. Westreich (U.S. Nuclear Regulatory Commission), "Review Criteria for Title 10 of the Code of Federal Regulations Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ADAMS Accession No. ML13295A467).

6.6. Letter from J. G. Lamb (USNRC) to B. C. Hanson (Exelon), "Oyster Creek Nuclear Generating Station - Issuance of Amendment Regarding Reactor Building Vital Area Access Control (TAC NO. MF3295)," dated March 30, 2015 (ADAMS Accession No. ML14329A625).

6.7. Letter from J. F. Rogge (USNRC) to M. J. Pacilio (Exelon), "Oyster Creek Nuclear Generating Station – NRC Security Inspection Report 05000219/2014405."

ATTACHMENT 2

Revision to Cyber Security Plan Milestone 8 Completion Date

Proposed Facility Operating License Change (Mark-Up)

Oyster Creek Nuclear Generating Station

Renewed Facility Operating License No. DPR-16

(4) Exelon Generation Company 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 27817 and 27822), and the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans[1], submitted by letter dated May 17, 2006, is entitled: "Oyster Creek Nuclear Generating Station Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, Revision 5." The set contains Safeguards Information protected under 10 CFR 73.21.

Exelon Generation Company 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 Exelon Generation Company CSP was approved by Renewed License Amendment No. 280 and modified by License Amendment No. ~~280~~ XXX, 288.

(5) Inspections of core spray spargers, piping and associated components will be performed in accordance with BWRVIP-18, "BWR Core Spray Internals Inspection and Flaw Evaluation Guidelines," as approved by NRC staff's Final Safety Evaluation Report dated December 2, 1999.

(6) Long Range Planning Program - Deleted

(7) Reactor Vessel Integrated Surveillance Program

Exelon Generation Company is authorized to revise the Updated Final Safety Analysis Report (UFSAR) to allow implementation of the Boiling Water Reactor Vessel and Internals Project reactor pressure vessel Integrated Surveillance Program as the basis for demonstrating compliance with the requirements of Appendix H to Title 10 of the *Code of Federal Regulations* Part 50, "Reactor Vessel Material Surveillance Program Requirements," as set forth in the licensee's application dated December 20, 2002, and as supplemented on May 30, September 10, and November 3, 2003.

All capsules in the reactor vessel that are removed and tested must meet the test procedures and reporting requirements of the most recent NRC-approved version of the Boiling Water Reactor Vessel and Internals Project Integrated Surveillance Program appropriate for the configuration of the specimens in the capsule. Any changes to the capsule withdrawal schedule, including spare capsules, must be approved by the NRC prior to implementation. All capsules placed in storage must be maintained for future insertion. Any changes to storage requirements must be approved by the NRC, as required by 10 CFR Part 50, Appendix H.

[1] The Training and Qualification Plan and Safeguards Contingency Plan are Appendices to the Security Plan.

ATTACHMENT 3

Revision to Cyber Security Plan Milestone 8 Completion Date

Revised Cyber Security Commitment

Oyster Creek Nuclear Generating Station

Renewed Facility Operating License No. DPR-16

Provided below is a revision to the Regulatory Commitment regarding the Cyber Security Plan Implementation Schedule for OCNGS. This Regulatory Commitment for the thirteen Exelon Nuclear Power Plants was previously submitted in the letter from David T. Gudger to the USNRC Document Control Desk, "License Amendment Request regarding the Cyber Security Plan Implementation Schedule for Milestone 8," dated August 29, 2014, and approved by the letter from B. Purnell (USNRC) to B. C. Hanson, (Exelon Generation Company, LLC), "Issuance of Amendments Revising the Completion Date for Milestone 8 of the Exelon Cyber Security Plan," dated July 30, 2015. The Regulatory Commitment for all the other twelve Exelon Nuclear Power Plants is not being revised by this amendment request. Deleted text is shown in ~~strikeout~~ and new text is shown is **bold**.

NOTE – For OCNGS Only

#	Implementation Milestone Regulatory Commitment	Completion Date	Basis	Commitment Type
8	Full implementation of Exelon Cyber Security Plan for all SSEP functions will be achieved.	No later than ~~December 31, 2017~~ **August 31, 2021**	~~By the completion date, Exelon 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 refuel outage for implementation~~. **The requested MS8 extension to August 31, 2021, is based on the notification to permanently cease operations at OCNGS, pursuant to 10 CFR 50.82(a)(1)(i), and additional time for OCNGS to submit and for the NRC to process a separate request for an amendment to remove the Facility Operating License Condition that requires implementation of the Cyber Security Plan.**	One-Time Action

ATTACHMENT 4

Revision to Cyber Security Plan Milestone 8 Completion Date

Revised Cyber Security Plan Implementation Schedule

Oyster Creek Nuclear Generating Station

Renewed Facility Operating License No. DPR-16

Provided below is a revision to the Exelon Cyber Security Implementation Plan Milestone 8 completion date for OCNGS. The implementation plan for the thirteen Exelon Nuclear Power Plants was previously submitted in the letter from David T. Gudger to the USNRC Document Control Desk, "License Amendment Request regarding the Cyber Security Plan Implementation Schedule for Milestone 8," dated August 29, 2014 and approved by the letter from B. Purnell (USNRC) to B. C. Hanson, (Exelon Generation Company, LLC), "Issuance of Amendments Revising the Completion Date for Milestone 8 of the Exelon Cyber Security Plan," dated July 30, 2015. The implementation plans for all the other twelve Exelon Nuclear Power Plants are not being revised by this amendment request.

NOTE – For OCNGS Only

#	Implementation Milestone Regulatory Commitment	Completion Date	Basis	Commitment Type
8	Full implementation of Exelon Cyber Security Plan for all SSEP functions will be achieved.	No later than August 31, 2021	The requested MS8 extension to August 31, 2021, is based on the notification to permanently cease operations at OCNGS, pursuant to 10 CFR 50.82(a)(1)(i), and additional time for OCNGS to submit and for the NRC to process a separate request for an amendment to remove the Facility Operating License Condition that requires implementation of the Cyber Security Plan.	One-Time Action