



ENERGY NORTHWEST

Dale K. Atkinson
Vice President, Operational Support
P.O. Box 968, PE03
Richland, WA 99352-0968
Ph. 509.377.4302 | F. 509.377.4098
dkatkinson@energy-northwest.com

July 22, 2010
GO2-10-098

10 CFR 73.54

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

**Subject: COLUMBIA GENERATING STATION, DOCKET NO. 50-397
REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING
STATION CYBER SECURITY PLAN**

- References:
- 1) Letter GO2-09-153 dated November 16, 2009, DK Atkinson (Energy Northwest) to NRC, "Request for Approval of the Columbia Generating Station Cyber Security Plan"
 - 2) NRC Letter dated May 24, 2010, CF Lyon (NRC) to JV Parrish (Energy Northwest), "Columbia Generating Station – License Amendment Request for Approval of the Cyber Security Plan (TAC No. ME2624)"
 - 3) NEI 08-09 Revision 6, "Cyber Security Plan for Nuclear Power Reactors," April 2010
 - 4) NRC Letter dated June 7, 2010, RP Correia (NRC) to CE Earls (NEI), "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template, Rev. 6'"

Dear Sir or Madam:

As requested in Reference 2, Energy Northwest hereby withdraws the Reference 1 Cyber Security Plan application and submits a revised Cyber Security Plan application based on Reference 3 with a Reference 4 definition for cyber attack.

In accordance with the provisions of Section §73.54 Title 10 of the Code of Federal Regulations (10 CFR) and Reference 2, Energy Northwest is submitting, as specified in §50.4 and §50.90, a request for an amendment to the Facility Operating License (FOL) for Columbia Generating Station (CGS). This proposed amendment requests Nuclear Regulatory Commission (NRC) approval of the CGS Cyber Security Plan, provides an Implementation Schedule, and proposes a revision to the existing FOL Physical Protection license condition 2.E to require Energy Northwest to fully implement and maintain in effect all provisions of the Commission approved CGS Cyber Security Plan.

800/A
NRC

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Page 2

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

- Attachment 1 provides a marked-up page showing the proposed FOL change.
- Attachment 2 provides the proposed FOL change in final typed format.

Enclosure 2 provides a copy of the CGS Cyber Security Plan which is a stand alone document that will be incorporated by reference into the CGS Physical Security Plan upon the staff's approval. Enclosure 3 provides a copy of the CGS Cyber Security Plan Implementation Schedule and describes commitments made in this submittal. Energy Northwest requests that Enclosure 2 and Enclosure 3, which contain security sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390.

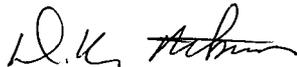
Enclosure 4 provides a table which lists the CGS Cyber Security Plan deviations from the Reference 3 template.

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

If you should have any questions regarding this submittal, please contact Mr. DW Gregoire at (509) 377-8616.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the date of this letter.

Respectfully,



DK Atkinson
Vice President, Operational Support

- Enclosures:
- 1) Evaluation of Proposed Change
 - 2) Cyber Security Plan for Columbia Generating Station (Security-Related Information – Withhold Under 10 CFR 2.390)
 - 3) Columbia Generating Station Cyber Security Plan Implementation Schedule (Security-Related Information – Withhold Under 10 CFR 2.390)
 - 4) Columbia Generating Station Deviations from NEI 08-09, Revision 6

cc: NRC RIV Regional Administrator
NRC NRR Project Manager
NRC Senior Resident Inspector/988C
RN Sherman – BPA/1399
WA Horin – Winston & Strawn
EFSEC Manager
RR Cowley – WDOH

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 1

Page 1 of 7

Evaluation of Proposed Change

Subject: Request for Approval of the Columbia Generating Station Cyber Security Plan

- 1.0 SUMMARY DESCRIPTION
 - 2.0 DETAILED DESCRIPTION
 - 3.0 TECHNICAL EVALUATION
 - 4.0 REGULATORY EVALUATION
 - 5.0 ENVIRONMENTAL CONSIDERATION
 - 6.0 REFERENCES
-

ATTACHMENTS

Attachment 1 – Marked-up Page Showing the Proposed FOL Change

Attachment 2 - Proposed FOL Change in Final Typed Format

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 1

Page 2 of 7

1.0 SUMMARY DESCRIPTION

The proposed license amendment request (LAR) includes the proposed Columbia Generating Station (CGS) Cyber Security Plan, an Implementation Schedule, and a proposed revision to the existing Facility Operating License (FOL) Physical Protection license condition.

2.0 DETAILED DESCRIPTION

The proposed LAR includes four parts: 1) the proposed Plan, 2) an Implementation Schedule, 3) a table listing deviations from Nuclear Energy Institute (NEI) 08-09, Revision 6 (Reference 3), and 4) a proposed revision to the existing FOL Physical Protection license condition 2.E to require Energy Northwest to fully implement and maintain in effect all provisions of the Commission approved CGS Cyber Security Plan as required by Section §73.54 of Title 10 of the Code of Federal Regulations (10 CFR). The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," (Rule) 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 final rule change published on March 27, 2009 (Reference 1).

3.0 TECHNICAL EVALUATION

Cyber security requirements are codified as new §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 are substantial improvements upon the requirements imposed by EA-02-026 (Reference 2).

The LAR includes the proposed Plan (Enclosure 2) that conforms to the template provided in Appendix A of NEI 08-09, Revision 6 and a table listing deviations from the template (Enclosure 4). In addition, the LAR includes the proposed revision to the existing FOL license condition for "Physical Protection" (Attachments 1 and 2). Finally, the LAR contains the proposed Implementation Schedule (Enclosure 3) as required by 10 CFR 73.54.

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

The 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 §50.4 and §50.90.

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 1

Page 3 of 7

4.2 Significant Hazards Consideration

Energy Northwest 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 FOL to implement and maintain a Cyber Security Plan as part of Energy Northwest's overall program for physical protection of CGS. Inclusion of the CGS Cyber Security Plan in the FOL itself does not involve any modifications to any safety-related structures, systems or components (SSCs). Rather, the CGS 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 CGS's digital computer and communications systems and networks are protected from cyber attacks. The CGS 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 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 analyzed?

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

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 1

Page 4 of 7

- 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, Energy Northwest 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

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 applicable regulations as identified herein, 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 CGS and will be a part of the Physical Security Plan. The proposed amendment would not change any requirements with respect to installation or use of a facility component located within CGS's restricted area, as defined in 10 CFR 20.1003. Accordingly, the proposed amendment does not involve: (1) a significant hazards consideration, (2) a significant change in the types or a significant increase in the amounts of any effluents that may be released offsite, or (3) a significant increase in individual or cumulative occupational radiation exposure. The proposed amendment meets the criteria for categorical exclusion in accordance with 10 CFR 51.22(c) and no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

**REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER
SECURITY PLAN**

Enclosure 1

Page 5 of 7

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, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002
3. NEI 08-09 Revision 6, "Cyber Security Plan for Nuclear Power Reactors," April 28, 2010

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 1

Page 6 of 7

Attachment 1 – Marked-up Page Showing the Proposed FOL Change

- 10 -

- D. Exemptions from certain requirements of Appendices G, H and J to 10 CFR Part 50, are described in the Safety Evaluation Report. These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, these exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of this exemption the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.
- E. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security plan, training and qualification plan, and safeguards contingency plan, 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 to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plan, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Columbia Generating Station Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Independent Spent Fuel Storage Installation Plan, Revision 3" submitted May 18, 2006.
- F. Deleted. **Add: Columbia Generating Station cyber security plan.**
- G. The licensee shall notify the Commission, as soon as possible but not later than one hour, of any accident at this facility which could result in an unplanned release of quantities of fission products in excess of allowable limits for normal operation established by the Commission.
- H. The licensee shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

Strike out "206"

Amendment No. ~~57,170,103~~ 206
Revised by letter dated February 2, 2007

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 1

Page 7 of 7

Attachment 2 - Proposed FOL Change in Final Typed Format

- 10 -

- D. Exemptions from certain requirements of Appendices G, H and J to 10 CFR Part 50, are described in the Safety Evaluation Report. These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, these exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of this exemption the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.
- E. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved Columbia Generating Station cyber security plan; physical security plan, training and qualification plan, and safeguards contingency plan, 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 to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plan, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Columbia Generating Station Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Independent Spent Fuel Storage Installation Plan, Revision 3" submitted May 18, 2006.
- F. Deleted.
- G. The licensee shall notify the Commission, as soon as possible but not later than one hour, of any accident at this facility which could result in an unplanned release of quantities of fission products in excess of allowable limits for normal operation established by the Commission.
- H. The licensee shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

REQUEST FOR APPROVAL OF THE COLUMBIA GENERATING STATION CYBER SECURITY PLAN

Enclosure 4

Page 1 of 1

Columbia Generating Station Deviations from NEI 08-09, Revision 6

NEI 08-09 Location	NEI 08-09 Wording	CGS Deviation
Appendix A, Section 1 1st Paragraph	[Site/Licensee] acknowledges that the implementation of this plan does not alleviate their responsibility to comply with other NRC regulations.	Energy Northwest acknowledges that the implementation of this plan does not alleviate responsibility to comply with other NRC regulations. Deleted the word "their" for grammatical correctness.
Appendix A, Section 1 3 rd Paragraph	A Glossary of terms used within this Plan and Appendices of NEI 08-09, Revision 6, is contained in Appendix B of NEI 08-09, Revision 6.	This wording has been replaced with the actual terms contained within NEI 08-09, Revision 6, Appendix B. CGS has elected to incorporate the definitions directly into the Cyber Security Plan.
Section 3.1.3 – 1 st Bullet	Refer to NEI 08-09, Revision 6, Appendix B, Glossary for definition of Critical System.	Refer to Section 1.3 for definition of Critical System. Maintains consistency of incorporating definitions directly.
Section 3.1.3 – 2 nd Bullet	Refer to NEI 08-09, Revision 6, Appendix B, Glossary for definition of Critical System.	Refer to Section 1.2 for definition of Critical Digital Asset. Maintains consistency of incorporating definitions directly.
Appendix B, "Cyber Attack"	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 SSEP function.	<p>This term has been added as Section 1.4 in the plan and the wording has been changed to read:</p> <p>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 CDA.</p> <p>Reference 1 below concluded that submission of the cyber security plan in accordance with NEI 08-09, Revision 6 with the exception of the definition of "cyber attack" would be acceptable. Reference 2 provided the above wording as an acceptable definition of "cyber attack" which has been incorporated as Section 1.4 in this plan.</p>

References: 1) NRC Letter dated May 24, 2010, CF Lyon (NRC) to JV Parrish (Energy Northwest), "Columbia Generating Station – License Amendment Request for Approval of the Cyber Security Plan (TAC No. ME2624)"

2) NRC Letter dated June 7, 2010, RP Correia (NRC) to CE Earls (NEI), "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template, Rev. 6'"