ENERGY NORTHWEST

Donald W. Gregoire
P.O. Box 968, PE20
Richland, WA 99352-0968
Ph. 509-377-8616 | F. 509-377-4317

GO2-14-105
June 19, 2014

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**
CYBER SECURITY PLAN – MILESTONES 1-7 COMPLETION STATUS

Reference: Letter GI2-13-140 dated August 12, 2013, NRC to ME Reddemann (Energy Northwest), "Columbia Generating Station, NRC Temporary Instruction 2201/004, 'Inspection of Implementation of Interim Cyber Security Milestones 1 – 7,' Inspection Report 05000397/2013406."

Dear Sir or Madam:

In accordance with a request in the Reference letter to provide written notification to the NRC's Regional Office when the corrective actions for the issues identified during the inspection have been completed, Energy Northwest (EN) is herewith submitting a status report on completion of those actions. The corrective actions directly resulting from the inspection and related to Milestones 1 through 7 completions as documented in multiple Condition Reports (CRs) identified in the inspection report (Reference) have been completed as documented in the attachment. Two other activities related to overall implementation of the Cyber Security Program and involving changes in the Control Room Network and assessment of the Digital Electro-Hydraulic (DEH) System are still in progress and have tentative scheduled completion dates for 2015 and 2017, respectively.

There are no new commitments being made to the NRC by this letter. Should you have any questions, please call JR Trautvetter at (509) 377-4337.

Respectfully,

J.R. Trautvetter

J.R. Trautvetter
Acting Manager, Regulatory Programs
for DW Gregoire
Manager, Regulatory Programs

Attachment – Columbia Generating Station Cyber Security Inspection 05000397/2013406 – Findings and Resolutions

cc: NRC Region IV Administrator
NRC NRR Project Manager
NRC Sr. Resident Inspector - 988C
MA Jones – BPA/1399
DE Sandlin – BPA/1399
WA Horin - Winston & Strawn

5001 A
NRR

CYBER SECURITY PLAN – MILESTONES 1-7 COMPLETION STATUS
Attachment

Columbia Generating Station Cyber Security Inspection 05000397/2013406 – Findings and Resolutions

Finding/Deficiency	Resolution	Tracking CR Number	Completion Status
Milestone 1: Establishment of a Cyber Security Assessment Team			
None	N/A	N/A	N/A
Milestone 2: Identification and Documentation of Critical Systems (CSs) and Critical Digital Assets (CDAs)			
A licensee identified violation of 10 CFR 73.54 was identified for the failure to adequately identify CDAs consistent with the requirements of Milestone 2 of the licensee's Cyber Security Plan (CSP).	Resolution of this finding to bring the program into compliance included the following activities: • Revised procedure SWP-CSW-18 to conform to the CSP • Initial subset of DAs was screened by CSAT • EP Field Team Kits included several DAs. Added as CDAs • Procedure changes and walkdowns were used to correct the CDA identification process • Revised procedure ISDI-CYBER-08 to incorporate new process for screening DAs	 00281324[a] 00281250[a] 00280653[a] 00282450[a] and 00282941[a] 00282235[a]	 Complete Complete Complete Complete Complete
Milestone 3: Installation of a Protective Device between Lower and Higher Security Levels			
None	Enhancements related to this milestone included: • Network connectivity to Engineering Test Lab was removed • Modified network access outside the PA	 00279442[a] 00282451[a]	 Complete Complete

Finding/Deficiency	Resolution	Tracking CR Number	Completion Status
Milestone 4: Implementation of Access Control for Portable and Mobile Devices			
Deficiencies in controlling access to a digital scanning device with external devices.	Resolution of this finding to bring the program into compliance included the following activities:		
	• Isolated scanning stations based on Industry OE	00280268[a]	Complete
	• Published location of scanning stations and added signage	00281557[a]	Complete
	• Added additional log reviews to department instruction	00282942[a]	Complete
	• OE on multiple scanning engines – no action necessary	00282943[a]	Complete
	• Procedure revised and cabinets changed out	00283117[a]	Complete
	• Configuration of scanning stations was locked down and details included in SWP-CSW-15	00283118[a]	Complete
	• Department instruction was developed for scanning station management	00283178[a]	Complete
	• Passwords were placed in a locked container	00283179[a]	Complete
	• Additional language was added to SWP-CSW-15 to document laptop controls	00283264[a]	Complete
	• Created report on Security Control Analysis	00283265[a] and 00283118[a]	Complete Complete
	• Assignments for CSP Milestone 4 issued	00283295[a]	Complete
	• Actions for Computer Engineering and I&C to generate tracking methodology	00283100[a], 00306411[b], and 00306876[b]	Complete Ongoing[e] Ongoing[e]

CYBER SECURITY PLAN – MILESTONES 1-7 COMPLETION STATUS
Attachment

Finding/Deficiency	Resolution	Tracking CR Number	Completion Status
Milestone 5: Observation and Identification of Obvious Cyber Related Tampering			
Non-cited violation associated with 10 CFR 73.54 for failure to fully implement required security controls.	Resolution of this finding to bring the program into compliance included the following activities: • Issued procedures ISDI-CYBER-17 and ISDI-CYBER-18 • Updated tamper training module to incorporate additional details within the training	00283250[a] and 00283251[a] 00283290[a]	Complete Complete Complete
Milestone 6: Implementation of Cyber Security Controls for CDAs that Could Adversely Impact the Design Function of Target Set Equipment			
Licensee identified violation of 10 CFR 73.54 for the failure to adequately identify CDAs that could adversely impact the design function of physical security target set equipment.	Resolution of this finding to bring the program into compliance included the following activities: • Revised procedure ISDI-CYBER-08 to incorporate new process for screening	00282235[a], 00280268[a], and 00282450[a]	Complete Complete Complete
Milestone 7: Implementation and Commencement of Ongoing Monitoring and Assessment Activities			
Non-cited violation of 10 CFR 73.54 for the failure to fully implement ongoing monitoring and assessment activities of the CSP implementation schedule.	Resolution of this finding to bring the program into compliance included the following activities: • Closed additional actions related to Milestones 5 and 7 • Published procedures ISDI-CYBER-17 and ISDI-CYBER-18	00283180[a] and 00283251[a]	Complete Complete

Finding/Deficiency	Resolution	Tracking CR Number	Completion Status
Other Activities Resulting From The Inspection			
N/A	• Apparent Cause on malicious software detected	00275206[a]	Complete
	• Follow up activities after publication of NRC Cyber Security guidance	00282450[a]	Complete
	• Enabled IPS on external firewall	00241815[a]	Complete
	• Resolved issues with Cyber CBT and corrective action	00192378[a]	Complete
	• Assessment of project impacts due to Cyber Security concerns	00218174[a]	Complete
	• Resolved issue with worm possibly affecting DEH System	00195762[a]	Complete
	• SCC computers were removed from an OU that required screen savers	00203869[a]	Complete
	• Computers scanned, cleaned, and hardened after discovery of malware on MOV computers	00280513[a]	Complete
	• Resolved Supervisor access issues for researching Cyber Security solutions	00280815[a]	Complete
	• In progress modification to Control Room network	00249961[a] and 00232205[b]	Ongoing[c] (Scheduled for completion in 2015) Ongoing[c]
	• DMA System assessment approved by CSAT	00244217[b]	Complete
	• The assessment of the DEH Digital Electro-Hydraulic ON System is in progress.	00244331[b]	Ongoing (Scheduled for completion in 2017)[d]

NOTES:

[a] Condition Reports listed in NRC Inspection Report 05000397/2013406 (Reference);

[b] Condition Reports not referenced in NRC Inspection Report 05000397/2013406 (Reference);

[c] ARs 00249961 and 00232205 are AR-EVAL (Evaluation) type Action Requests and are scheduled for completion in 2015. These are not Condition Reports and have no corrective actions. AR 00249961 tracks a cyber security modification that was generated as a part of Milestone 8 completion and not Milestones 1-7. The inspector requested to review this documentation during the inspection and it is listed in the inspection report. However, it is not in CAP;

[d] AR 244331 is an AR-ITSR (Information Technology Service Request) type Action Request. It is not a Condition Report and has no corrective actions. This AR conducts a cyber security assessment of the DEH (Digital Electro-Hydraulic) System;

[e] ARs 00306411 and 00306876 are yearly re-occurring Model ARs that will get a new number every year. These ARs are SELF (self-managed) type assignments for internal tracking of Quarterly Walk downs and password changes and will be on an "ongoing" basis during the year and will be closed at the end of each year.

[f] Condition Report 00282480 is cited in NRC Inspection Report 05000397/2013406, page 17 (Reference) but is not included in table because it is not related to the Columbia Cyber Security Inspection (suspected typographical error).