UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 27, 2015

Mr. Mark E. Reddemann
Chief Executive Officer
Energy Northwest
P.O. Box 968 (Mail Drop 1023)
Richland, WA 99352-0968

SUBJECT: COLUMBIA GENERATING STATION - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE REVISION (TAC NO. MF4387)

Dear Mr. Reddemann:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 231 to Renewed Facility Operating License No. NPF-21 for Columbia Generating Station. The amendment consists of changes to the physical protection license condition in response to your application dated June 25, 2014. The amendment revises the Columbia Generating Station Cyber Security Plan (CSP) Milestone 8 full implementation date as set forth in the CSP Implementation Schedule.

A copy of the related Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

Andrea E. George, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-397

Enclosures:
1. Amendment No. 231 to NPF-21
2. Safety Evaluation

cc w/encls: Distribution via Listserv

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

ENERGY NORTHWEST

DOCKET NO. 50-397

COLUMBIA GENERATING STATION

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 231
License No. NPF-21

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment by Energy Northwest (licensee), dated June 25, 2014, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act) and the Commission's regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and Paragraph 2.E of Renewed Facility Operating License No. NPF-21 is hereby amended to read as follows:

> The licensee 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 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." Energy Northwest 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 Energy Northwest CSP and associated Implementation Schedule were approved by License Amendment No. 222, and the Implementation Schedule was revised by License Amendment No. 231.

3. The license amendment is effective as of its date of issuance and shall be implemented within 30 days from the date of issuance.

FOR THE NUCLEAR REGULATORY COMMISSION

Michael T. Markley, Chief
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Renewed Facility
Operating License No. NPF-21

Date of Issuance: March 27, 2015

ATTACHMENT TO LICENSE AMENDMENT NO. 231

RENEWED FACILITY OPERATING LICENSE NO. NPF-21

DOCKET NO. 50-397

Replace the following page of the Renewed Facility Operating License No. NPF-21 with the attached revised page. The revised page is identified by amendment number and contains vertical lines indicating the areas of change.

Facility Operating License

REMOVE	INSERT
-9-	-9-

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, 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 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." Energy Northwest 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 Energy Northwest CSP and associated Implementation Schedule were approved by License Amendment No. 222, and the Implementation Schedule was revised by License Amendment No. 231.

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.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 231 TO

RENEWED FACILITY OPERATING LICENSE NO. NPF-21

ENERGY NORTHWEST

COLUMBIA GENERATING STATION

DOCKET NO. 50-397

1.0 INTRODUCTION

By application dated June 25, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14188C091), Energy Northwest (the licensee) requested changes to the Renewed Facility Operating License (FOL) for Columbia Generating Station (CGS). The proposed change would revise the date of Cyber Security Plan (CSP) Implementation Schedule Milestone 8 and the existing physical protection license condition in the Renewed FOL. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP.

Portions of the letter dated June 25, 2014, contain sensitive unclassified non-safeguards information and, accordingly, those portions are withheld from public disclosure in accordance with the provisions of paragraph 2.390(d)(1) of Title 10 of the *Code of Federal Regulations* (10 CFR).

2.0 REGULATORY EVALUATION

The U.S. Nuclear Regulatory Commission (NRC) staff reviewed and approved the licensee's existing CSP implementation schedule by License Amendment No. 222 dated July 27, 2011 (ADAMS Accession No. ML111740223). The approved amendment incorporated the CSP into the facility's current licensing basis via revision to the physical protection license condition. The NRC staff considered the following regulatory requirements and guidance in its review of the current license amendment request (LAR) to modify the existing CSP implementation schedule:

- Title 10 to the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of digital computer and communication systems and networks," which states, in part, that: "Each [CSP] submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule."

- The licensee's Renewed FOL includes a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.

- In a publically available NRC memorandum dated October 24, 2013 (ADAMS Accession No. ML13295A467), "Review Criteria for Title 10 of the *Code of Federal Regulations* Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," the NRC staff listed criteria to consider during evaluations of licensees' requests to postpone their cyber security program implementation date (commonly known as Milestone 8).

The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensee, particularly in light of the regulatory requirement at 10 CFR 73.54, that "[i]mplementation of the licensee's cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (ADAMS Accession No. ML110980538), the implementation of the plan, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule, therefore, will require prior NRC approval as required by 10 CFR 50.90.

3.0 TECHNICAL EVALUATION

Background information regarding Cyber Security Implementation Plans and a description of each Milestone can be found in the Nuclear Energy Institute (NEI) letter dated February 28, 2011, "Template for the Cyber Security Plan Implementation Schedule" (ADAMS Package Accession No. ML110600206).

3.1 Licensee's Requested Change

Amendment No. 222 to FOL NPF-21 for CGS was issued on July 27, 2011. The NRC staff also approved the licensee's CSP implementation schedule, as discussed in the Safety Evaluation (SE) issued with the amendment. The implementation schedule had been submitted by the licensee based on the template prepared by NEI, which the NRC staff found acceptable for licensees to use to develop their CSP implementation schedules by letter dated March 1, 2011 (ADAMS Accession No. ML110070348). The licensee's proposed implementation schedule for the CSP identified completion dates and bases for the following eight milestones:

1) Establish the Cyber Security Assessment Team (CSAT);

2) Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);

3) Implement installation of a deterministic one-way device between lower level devices and higher level devices;

4) Implement the security control "Access Control For Portable And Mobile Devices;"

5) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;

6) Identify, document, and implement cyber security controls in accordance with *Mitigation of Vulnerabilities and Application of Cyber Security Controls* for CDAs that could adversely impact the design function of physical security target set equipment;

7) Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and

8) Fully implement the CSP.

Currently, Milestone 8 of the CGS CSP requires the licensee to fully implement the CSP by December 31, 2015. In its June 25, 2014, application, the licensee proposed to change the Milestone 8 completion date to December 31, 2017.

The licensee provided the following information pertinent to each of the criteria identified in the NRC memorandum dated October 24, 2013, regarding guidance for submitting CSP Milestone 8 implementation date revision license amendment requests (see Section 2.0 of this SE for more information):

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

The licensee stated that the specific CSP requirement requiring additional time to implement is CSP Section 3.1, *Analyzing Digital Computer Systems and Networks and Applying Security Controls*. The licensee provided a list of specific requirements in CSP Section 3.1 needing additional time.

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

The licensee stated that despite a project team of nine full-time equivalent staff and two engineering firms contracted to perform several CSP modification conceptual studies, Energy Northwest is experiencing challenges with full implementation of Milestone 8. In its LAR, the licensee stated, in part, that:

> Hundreds of security controls must be addressed for each of the 1,500 CDAs. Each assessment package is then reviewed and approved by the Cyber Security Assessment Team. Despite the project team size, the rate of completion of CDA assessments combined with the standard timeline for the resulting engineering design change and implementation package does not support Milestone 8 completion by the current completion date.

The licensee further stated in its LAR that it underestimated the level of effort necessary to address security controls, given that: (1) security control modifications are unique and new to

the plant and suppliers, (2) plant modifications must be carefully planned, scheduled, and implemented to ensure they do not impact plant safety and operation, resulting in additional time to assure safety; and (3) suppliers release products that have not been adequately documented and tested that result in corrective action investigations, delays, and resource drains.

In its LAR, the licensee provided detailed information and justification regarding the need for additional time to fully implement the CGS CSP, including the following: (1) need for resolution of NEI/NRC discussion on CDA scope/security controls; (2) need for defining the cyber security controls in NEI 08-09, Revision 6; (3) need to complete the resource-intensive CDA assessments, (4) increased time for planning, scheduling, and implementation remediation activities; (5) need for managing change efforts across diverse organizations; and (6) required training on new programs, processes, and procedures. Regarding the need to manage change efforts across diverse organizations, the licensee provided, in part, the following information in its LAR:

- Cyber security must be integrated into day-to-day plant operations, maintenance, engineering, and procurement activities. This involves additional time for familiarizing the affected organizations with the new requirements. This process may involve several iterations.

- Integration of cyber security controls is taking longer than expected due to impacts on the work control process and maintenance activities.

- The added burden on the Maintenance department to address cyber security controls results in more time being needed to assure integrity during maintenance work on CDAs.

- Maintenance on CDAs must be performed by trained and qualified technicians. Integration of cyber security considerations into training materials has impacted all of the Maintenance disciplines.

- The Cyber Security team has spent significantly more time than expected assisting impacted organizations in understanding the new requirements and incorporating cyber security into each department's procedures, processes, and long-range planning.

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

In its LAR dated June 25, 2014, the licensee proposed a Milestone 8 completion date of December 31, 2017. The licensee also stated that changing the completion date of Milestone 8 will encompass one additional refueling outage and will provide adequate time to plan and schedule the implementation of design changes identified as a result of the CDA assessments.

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.

In its LAR dated June 25, 2014, the licensee stated that

> The completed cyber security implementation activities and the in-progress activities having a planned completion date of December 31, 2015, will provide assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks during implementation of the remainder of the program by the proposed Milestone 8 completion date of December 31, 2017.

The licensee provided details on the completed activities for each milestone. The licensee completed the implementation of interim Milestones 1 through 7. The licensee stated that these activities provide a high degree of protection against cyber security attacks during the time in which the licensee is implementing their full program.

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

In its LAR dated June 25, 2014, the licensee stated the following

> The Energy Northwest methodology for prioritizing Milestone 8 activities is centered on safety, security, [emergency preparedness (SSEP)], and [Balance of plant (BOP)] continuity of power considerations. The methodology is based on defense in depth, the installed configuration of the CDAs, and susceptibility to the five commonly identified threat vectors listed in the NRC Cyber Security significance determination process. As shown in the following hierarchy, prioritization for the CDA assessment begins with safety related CDAs and continues through the lower priority non-safety and [emergency preparedness] CDAs:
>
> - Safety Related CDAs.
> - Physical Security CDAs.
> - Important to Safety CDAs (including BOP CDAs that directly impact continuity of power) and control system CDAs.
> - Non-Safety related CDAs and Emergency Preparedness CDAs.

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

In its LAR dated June 25, 2014, the licensee provided technical details and positive results from implementation of three of the milestones.

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

The licensee provided, in part, the following information in its LAR dated June 25, 2014:

> Energy Northwest uses the site CAP to document cyber issues in order to trend, correct, and improve compliance with the Columbia CSP. The CAP database documents and tracks, from initiation through closure, all cyber security required actions including issues identified during ongoing program assessment activities. Adverse trends are monitored for program improvement and addressed via the CAP process.

The licensee listed examples of cyber security program issues and activities in the CAP.

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

The licensee provided a discussion of completed modifications. Additionally, the licensee stated that it has approved a long-range plan for cyber security modifications and that the extent of the modifications is dependent on final resolution of ongoing discussions between NEI and NRC regarding control application and scope. The licensee also stated that the engineering change process is being used to develop designs for multiple plant systems as defined by the 10 CFR 73.54 focus on SSEP. These designs are currently being scheduled around two outages (prior to the requested Milestone 8 date), with online changes scheduled per the regular work management process upon design completion.

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and the guidance in Section 2.0 of this SE. The NRC staff's evaluation is below.

The NRC staff concludes that the actions the licensee noted as requiring additional time to implement, contained in CSP Section 3.1., *Analyzing Digital Computer Systems and Networks and Applying Security Controls*, are reasonable as discussed below.

In its LAR dated June 25, 2014, the licensee indicated that completion of the activities associated with the CSP, as described in Milestones 1 through 7, and completed prior to December 31, 2012, will provide a high degree of protection against cyber attacks. The licensee detailed activities completed for each milestone and noted that several elements of Milestone 8 have already been implemented or will be implemented by the original Milestone 8 date of December 31, 2015. The NRC staff concludes that CGS is more secure after implementation of Milestones 1 through 7 because the activities that the licensee has completed mitigate the most significant cyber-attack vectors for the most significant CDAs. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 31, 2017, will provide adequate protection of the public health and safety and the common defense and security.

The licensee stated that despite a project team of nine full-time equivalent staff and two engineering firms contracted, it is experiencing challenges with full implementation of Milestone 8. For example, hundreds of security controls must be addressed for each of the 1500 CDAs. Despite the project team size, the rate of completion of CDA assessments combined with the standard timeline for the resulting engineering design change and implementation package does not support Milestone 8 completion by the current completion date. The NRC staff recognizes that CDA assessment work is much more complex and resource-intensive than originally anticipated, in part, due to the NRC expanding the scope of the cyber security requirements to include balance of plant. As a result, the licensee has a large number of additional tasks not originally considered when developing its CSP implementation schedule. The NRC staff concludes that the licensee's request for additional time to implement Milestone 8 is reasonable given the unanticipated complexity, volume, and scope of the work required to come into full compliance with its CSP.

The licensee proposed a Milestone 8 completion date of December 31, 2017. The licensee stated that changing the completion date of Milestone 8 allows for one additional refueling outage to methodically plan and schedule the implementation of design changes identified as a result of CDA assessments. The licensee stated its methodology for prioritizing Milestone 8 activities is centered on SSEP and BOP continuity of power considerations. The licensee stated that its methodology is based on defense in depth, the installed configuration of the CDAs, and susceptibility to commonly identified threat vectors. The NRC staff concludes, based on the large number of digital assets described above and the limited number of resources with the appropriate expertise to perform these activities, that the licensee's methodology for prioritizing work on CDAs is appropriate. The NRC staff further concludes that the licensee's request to delay final implementation of the CSP until December 31, 2017, is reasonable given the complexity of the remaining unanticipated work and the need to perform certain work, including design changes, during scheduled fuel outages.

3.3 Revision to License Condition

By letter dated June 25, 2014, the licensee proposed to modify Paragraph 2.E of Renewed FOL No. NPF-21, which provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP.

The license condition in Paragraph 2.E of Renewed FOL No. NPF-21 for CGS is modified as follows:

> The licensee 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 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." Energy Northwest 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 Energy Northwest CSP and associated Implementation Schedule were approved by License Amendment No. 222, and the Implementation Schedule was revised by License Amendment No. 231.

3.4 NRC Staff Conclusion

The NRC staff concludes that the licensee's request to delay full implementation of its CSP until December 31, 2017, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 provides mitigation for significant cyber-attack vectors for the most significant CDAs as discussed in the staff conclusion above; (ii) the scope of the work required to come into full compliance with the CSP implementation schedule was much more complicated than anticipated and not reasonably foreseeable; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule.

Based on its review of the licensee's submission, the NRC staff concludes that the licensee's implementation of Milestones 1 through 7 adds significant protection against cyber attacks; that the licensee's explanation of the need for additional time is compelling; and that it is acceptable for Energy Northwest to complete implementation of Milestone 8, full implementation of the CSP by December 31, 2017. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 31, 2017 will provide adequate protection of the public health and safety and the common defense and security. The NRC staff also concludes that, upon full implementation of the licensee's CSP, the requirements of the licensee's CSP and 10 CFR 73.54 will be met. Therefore, the NRC staff concludes that proposed change to the CSP full implementation schedule is acceptable.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the appropriate Washington State official was notified of the proposed issuance of the amendment. The State official had no comments.

5.0 ENVIRONMENTAL CONSIDERATION

This is an amendment of a 10 CFR Part 50 license that relates solely to safeguards matters and does not involve any significant construction impacts. This amendment is an administrative change to extend the date by which the licensee must have its CSP fully implemented. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(12). 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 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that 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.

Principal Contributor: J. Rycyna, NSIR

Date: March 27, 2015.

March 27, 2015

Mr. Mark E. Reddemann
Chief Executive Officer
Energy Northwest
P.O. Box 968 (Mail Drop 1023)
Richland, WA 99352-0968

SUBJECT: COLUMBIA GENERATING STATION - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE REVISION (TAC NO. MF4387)

Dear Mr. Reddemann:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 231 to Renewed Facility Operating License No. NPF-21 for Columbia Generating Station. The amendment consists of changes to the physical protection license condition in response to your application dated June 25, 2014. The amendment revises the Columbia Generating Station Cyber Security Plan (CSP) Milestone 8 full implementation date as set forth in the CSP Implementation Schedule.

A copy of the related Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,
/RA/

Andrea E. George, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-397

Enclosures:
1. Amendment No. 231 to NPF-21
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL4-1 Reading
RidsAcrsAcnw_MailCTR Resource
RidsNsirOd Resource
RidsNrrDorlDpr Resource
RidsNrrDorlLpl4-1 Resource
RidsNrrPMColumbia Resource
RidsNrrLAJBurkhardt Resource
RidsRgn4MailCenter Resource
JRycyna, NSIR

ADAMS Accession No.: ML15042A464 *via email

OFFICE	NRR/DORL/LPL4-1/PM	NRR/DORL/LPL4-1/LA	NSIR/CSD/D
NAME	AGeorge	JBurkhardt	RFelts*
DATE	2/18/15	2/13/15	2/9/15
OFFICE	OGC – NLO	NRR/DORL/LPL4-1/BC	NRR/DORL/LPL4-1/PM
NAME	SFowler*	MMarkley	AGeorge
DATE	3/26/15	3/27/15	3/27/15

OFFICIAL RECORD COPY