



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

November 19, 2015

Mr. Louis P. Cortopassi
Site Vice President and Chief Nuclear Officer
Omaha Public Power District
Fort Calhoun Station
9610 Power Lane, Mail Stop FC-2-4
Blair, NE 68008

SUBJECT: FORT CALHOUN STATION, UNIT NO. 1 - ISSUANCE OF AMENDMENT RE:
REVISION TO CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE
COMPLETION DATE (CAC NO. MF5854)

Dear Mr. Cortopassi:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 284 to Renewed Facility Operating License No. DPR-40 for the Fort Calhoun Station, Unit No. 1. The amendment consists of changes to the operating license in response to your application dated November 25, 2014. You provided a redacted version of your application by letter dated April 20, 2015.

The amendment revises the Cyber Security Plan (CSP) Implementation Milestone 8 completion date and the physical protection license condition, by extending the CSP Milestone 8 full implementation date from December 31, 2015, to December 31, 2017.

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

Sincerely,

A handwritten signature in black ink that reads "CFLyon".

Carl F. Lyon, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-285

Enclosures:

1. Amendment No. 284 to DPR-40
2. Safety Evaluation

cc w/encls: Distribution via Listserv



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

OMAHA PUBLIC POWER DISTRICT

DOCKET NO. 50-285

FORT CALHOUN STATION, UNIT NO. 1

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 284
Renewed License No. DPR-40

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment by the Omaha Public Power District (the licensee), dated November 25, 2014, with a redacted version of the application provided by letter dated April 20, 2015, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and 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 license 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.

Enclosure 1

2. Accordingly, the license is amended by changes to paragraphs 3.B. and 3.C. of Renewed Facility Operating License No. DPR-40.

Paragraph 3.B. is hereby amended to read as follows:

B. Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 284, are hereby incorporated in the license. Omaha Public Power District shall operate the facility in accordance with the Technical Specifications.

Paragraph 3.C. is hereby amended to read as follows:

C. Security and Safeguards Contingency Plans

The Omaha Public Power District 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 plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Fort Calhoun Station Security Plan, Training and Qualification Plan, Safeguards Contingency Plan," submitted by letter dated May 19, 2006.

OPPD 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 OPPD CSP was approved by License Amendment No. 266 and modified by License Amendment No. 284.

3. The license amendment is effective as of its date of issuance and shall be implemented within 60 days of the date of issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on November 25, 2014, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Robert J. Pascarelli, 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. DPR-40

Date of Issuance: November 19, 2015

ATTACHMENT TO LICENSE AMENDMENT NO. 285

RENEWED FACILITY OPERATING LICENSE NO. DPR-40

DOCKET NO. 50-285

Replace the following page of the Renewed Facility Operating License No. DPR-40 with the attached revised page. The revised page is identified by amendment number and contains vertical lines indicating the areas of change.

License Page

REMOVE

INSERT

-3-

-3-

- (4) Pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess, and use in amounts as required any byproduct, source, or special nuclear material without restriction to chemical or physical form for sample analysis or instrument calibration or when associated with radioactive apparatus or components;
 - (5) Pursuant to the Act and 10 CFR Parts 30 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by operation of the facility.
 3. This renewed license shall be deemed to contain and is subject to the conditions specified in the following Commission regulations in 10 CFR Chapter I: Part 20, Section 30.34 of Part 30, Section 40.41 of Part 40, Section 50.54 and 50.59 of Part 50, and Section 70.32 of Part 70; and is, subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:
 - A. Maximum Power Level

Omaha Public Power District is authorized to operate the Fort Calhoun Station, Unit 1, at steady state reactor core power levels not in excess of 1500 megawatts thermal (rate power).
 - B. Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 284 are hereby incorporated in the license. Omaha Public Power District shall operate the facility in accordance with the Technical Specifications.
 - C. Security and Safeguards Contingency Plans

The Omaha Public Power District 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 plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Fort Calhoun Station Security Plan, Training and Qualification Plan, Safeguards Contingency Plan," submitted by letter dated May 19, 2006.

OPPD 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 OPPD CSP was approved by License Amendment No. 266 and modified by License Amendment No. 284.



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 284 TO RENEWED FACILITY

OPERATING LICENSE NO. DPR-40

OMAHA PUBLIC POWER DISTRICT

FORT CALHOUN STATION, UNIT NO. 1

DOCKET NO. 50-285

1.0 INTRODUCTION

By application dated November 25, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15070A007), Omaha Public Power District (OPPD or the licensee) requested a change to the renewed facility operating license for the Fort Calhoun Station (FCS). The proposed change would revise the date of Cyber Security Plan (CSP) Implementation Schedule Milestone 8, and the existing license conditions in the facility operating licenses. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP.

Portions of the letter dated November 25, 2014, contain sensitive unclassified non-safeguards information and, are withheld from public disclosure in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 2.390(d)(1). OPPD provided a redacted version of the application by letter dated April 20, 2015 (ADAMS Accession No. ML15110A420).

2.0 REGULATORY EVALUATION

The U.S. Nuclear Regulatory Commission (NRC or the Commission) staff reviewed and approved the licensee's existing CSP implementation schedule by FCS License Amendment No. 266 dated July 27, 2011 (ADAMS Accession No. ML111801094), concurrent with the incorporation of the CSP into the facility's current licensing basis. 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 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and networks," 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 facility operating license includes a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.

In a publicly-available NRC memorandum dated October 24, 2013 (ADAMS Accession No. ML13295A467), 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, thus, will require prior NRC approval as required by 10 CFR 50.90.

3.0 TECHNICAL EVALUATION

Amendment No. 266 to Renewed Facility Operating License (FOL) DPR-40 for FCS was issued on July 27, 2011. The NRC staff also approved the licensee's CSP implementation schedule, as discussed in the safety evaluation issued with the amendment. The implementation schedule had been submitted by the licensee based on a template prepared by the Nuclear Energy Institute (NEI) (ADAMS Accession No. ML110600218), which the NRC staff found acceptable for licensees to use to develop their CSP implementation schedules (ADAMS Accession No. ML110070348). The licensee's proposed implementation schedule for the CSP identified completion dates and bases for the following eight milestones:

- a) Establish the Cyber Security Assessment Team (CSAT);
- b) Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);
- c) Install a deterministic one-way device between lower level devices and higher level devices;
- d) Implement the security control "Access Control for Portable and Mobile Devices";
- e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;
- f) Identify, document, and implement technical 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;

- g) Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and
- h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

3.1 Licensee's Proposed Change

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

3.2 NRC Staff Evaluation

The cyber security implementation schedule demonstrates the licensee's ongoing implementation of its CSP prior to full implementation. For OPPD, the date for full implementation is specified by Milestone 8. CSP implementation activities include establishing a CSAT, identifying CSs and CDAs, installing deterministic one-way devices between defensive levels, implementing access control for portable and mobile devices, implementing methods to observe and identify obvious cyber related tampering, and conducting ongoing monitoring and assessment activities for target set CDAs. In their aggregate, the interim milestones demonstrate ongoing implementation of the CSP.

The importance of ongoing implementation is reflected in the NRC staff's October 24, 2013, guidance for considering requests to postpone the CSP full implementation date. The criteria in the guidance are:

- 1) Identification of the specific requirement or requirements of the cyber security plan that the licensee needs additional time to implement.
- 2) Detailed justification that describes the reason the licensee requires additional time to implement the specific requirement or requirements identified.
- 3) A proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.
- 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.
- 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.
- 6) A discussion of the licensee's cyber security program performance up to the date of the license amendment request.

- 7) A discussion of cyber security issues pending in the licensee's corrective action program.
- 8) A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

The licensee submitted its application on November 25, 2014, after the NRC staff issued the guidance. The licensee's application addressed each of the criteria in the guidance. The NRC staff has evaluated the licensee's application addressing the above criteria in its submittal dated November 25, 2014. The NRC staff's evaluation is below, numbered to match the criteria above.

- 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 it needs additional time to implement CSP Section 3.1.6, "*Mitigation of Vulnerabilities and Application of Cyber Security Controls*." The licensee identified the challenges to completing implementation of the CSP requirement.

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

The licensee noted that there are ongoing issues that need resolution prior to completing implementation of CSP Section 3.1.6. These include CDA assessment; remediation activities; change management; and training on new processes, procedures, and programs. The licensee stated it is experiencing significant challenges with full implementation of Milestone 8. The large number of CDAs within the FCS / OPPD program, in concert with the deterministic process required by CSP Section 3.1.6 has resulted in a much larger volume of assessment work than originally anticipated. In aggregate, the changes in the assessment and remediation process since 2010 have necessitated significant changes to the FCS CDA assessment methodology, changes to approved procedures, and the introduction of new methods not previously considered. These changes have required substantial resources to implement and re-performance of completed assessment activities. Although the precise scope of modifications cannot be conclusively articulated until the assessment process is complete and full program implementation is expected to require technically complex modifications. In most cases, the modifications would require refueling outages for safe implementation and must be coordinated with outage schedules and tested thoroughly prior to installation to confirm proper operation.

The NRC staff acknowledges implementation issues with large numbers of CDAs and the need to address many controls for each. Based on the information provided by the licensee in its application, the NRC staff believes that FCS would not be able to fully implement its CSP by December 31, 2015. The NRC staff recognizes that CDA assessment work is resource-intensive and that the licensee has a large number of CDAs. The NRC staff agrees remediation activities must be carefully considered and that working with security controls is a new experience for the licensee staff and suppliers, and that security modifications must be implemented to not impact safety and operations. The NRC staff understands that cyber

security program implementation has created change management challenges as it has impacted many aspects of the licensee's plant processes. In conclusion, the NRC staff finds the licensee's explanation of the need for additional time compelling, given the unanticipated complexity and scope of the work required to come into full compliance with its CSP.

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

The licensee proposed a Milestone 8 completion date of December 31, 2017, and stated the revised Milestone 8 date will encompass an additional refueling outage, which will provide more time to plan and schedule the implementation of design changes identified as a result of the CDA assessments.

Based on the licensee's application, the NRC staff concludes that delaying final implementation of the cyber security program will provide an opportunity to complete the work safely during the outage.

- 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.

The licensee indicated it was secure based on the cyber security implementation activities already completed. It then detailed the activities completed in each of the Milestones 1 through 7. The activities address significant cyber-attack vectors and applied controls to the most significant CDAs. Additionally, it is important to note that the delay of Milestone 8 does not affect the effectiveness of the completed activities.

The NRC staff concludes that the licensee's site is much more secure because the controls the licensee put in place mitigate the most significant cyber-attack vectors for the most significant CDAs.

- 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.

The licensee stated that its methodology for prioritizing Milestone 8 activities is predicated on completing CDA assessments and determining where vulnerabilities may exist. Prioritization of CDA assessments will be made on significant safety, security, or emergency preparedness consequences and equipment important to safety. Any resulting remedial modifications are then prioritized through the significance level and work control process. The FCS cyber-related activities are prioritized to first complete priority CDA assessments and then to identify and implement modifications required for remediation activities.

The NRC staff finds that based on the large number of digital assets described above, and the limited resources to perform these activities, the licensee's methodology for prioritizing work on CDAs is logical, conservative, and appropriate.

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

The licensee stated that a Nuclear Oversight audit of CSP Milestones 1 through 7 and on-going Quality Assurance surveillances under the physical security surveillance program have concluded that OPPD has an effective program at FCS. Issues identified during the audit were entered into the Corrective Actions Program (CAP) and addressed for improvement of the cyber security program. Also, OPPD has completed a comprehensive peer-assessment for Milestones 1 through 7 to ensure completeness and effectiveness of the implemented actions. Issues identified during the peer-assessment were entered into the CAP and addressed for improvement of the cyber security program. The NRC completed a cyber-security inspection at FCS, which resulted in three findings of very low significance (NRC Inspection Report 05000285/2014405, dated June 25, 2014, security-related information withheld from public availability in accordance with 10 CFR 2.390(d)(1); ADAMS Accession No. ML14176B202). Two of the identified findings have been remediated and the third finding is scheduled for remediation; these findings and their remediation are appropriately documented in the licensee's corrective action program. The independent Nuclear Safety Review Board comprised of senior managers and industry experts periodically reviews the FCS/OPPD CSP. In addition, ongoing monitoring and time-based periodic actions provide continuing program performance monitoring.

The NRC staff finds that the licensee's completion of Milestones 1 through 7 provides significant protection against cyber attacks. NRC staff concludes that the licensee is using the quality tools at its disposal to verify the effectiveness of the cyber security program and addressing issues in its corrective action program.

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

The licensee stated that the OPPD CAP is used to document all cyber security issues in order to trend, correct, and improve the FCS/OPPD CSP. The CAP database documents and tracks all cyber security required actions from Condition Report (CR) initiation to CR closure, including issues identified during ongoing program assessment activities. Adverse trends are monitored for CSP improvement and are addressed via the CAP process. The licensee listed examples of CSP issues and activities pending in the CAP.

The NRC staff finds that the examples reflect the evolution and implementation of the cyber security program and reinforce the licensee discussions above. The NRC staff concludes that the licensee is using the quality tools at its disposal to verify the effectiveness of the cyber security program and is addressing issues in its corrective action program.

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

The licensee provided a discussion of completed modifications and pending modifications. These are consistent with the discussions provided above and the licensee's CSP.

3.3 Revision to License Condition

By letter dated November 25, 2014, the licensee proposed to modify paragraph 3.C. of Renewed FOL No. DPR-40 for FCS that provides a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP.

Accordingly, the license condition in paragraph 3.C. of Renewed FOL No. DPR-40 for FCS is revised as follows:

C. Security and Safeguards Contingency Plans

The Omaha Public Power District 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 plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Fort Calhoun Station Security Plan, Training and Qualification Plan, Safeguards Contingency Plan," submitted by letter dated May 19, 2006.

OPPD 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 OPPD CSP was approved by License Amendment No. 266 and modified by License Amendment No. 284.

3.4 NRC Staff Conclusion

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

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the appropriate Nebraska State official, Ms. J. Schmitt, was notified on October 23, 2015, of the proposed issuance of the amendment. The State official had no comments.

5.0 ENVIRONMENTAL CONSIDERATION

This is an amendment to a 10 CFR Part 50 license that relates solely to safeguard 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)(ii). 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/CSD

Date: November 19, 2015

November 19, 2015

Mr. Louis P. Cortopassi
Site Vice President and Chief Nuclear Officer
Omaha Public Power District
Fort Calhoun Station
9610 Power Lane, Mail Stop FC-2-4
Blair, NE 68008

SUBJECT: FORT CALHOUN STATION, UNIT NO. 1 - ISSUANCE OF AMENDMENT RE:
REVISION TO CYBER SECURITY PLAN IMPLEMENTATION SCHEDULE
COMPLETION DATE (CAC NO. MF5854)

Dear Mr. Cortopassi:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 284 to Renewed Facility Operating License No. DPR-40 for the Fort Calhoun Station, Unit No. 1. The amendment consists of changes to the operating license in response to your application dated November 25, 2014. You provided a redacted version of your application by letter dated April 20, 2015.

The amendment revises the Cyber Security Plan (CSP) Implementation Milestone 8 completion date and the physical protection license condition, by extending the CSP Milestone 8 full implementation date from December 31, 2015, to December 31, 2017.

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

Sincerely,

/RA/
Carl F. Lyon, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-285

Enclosures:

1. Amendment No. 284 to DPR-40
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC

LPL4-1 Reading
RidsACRS_MailCTR Resource
RidsNrrDorlDpr Resource

RidsNrrDorlLpl4-1 Resource
RidsNrrPMFortCalhoun Resource
RidsNrrLAJBurkhardt Resource
RidsRgn4MailCenter Resource

JRycyna, NSIR/CSD
RFelts, NSIR/CSD
JAndersen, NSIR/CSD

ADAMS Accession No. ML15294A279 *email dated

OFFICE	NRR/DORL/LPL4-1/PM	NRR/DORL/LPL4-1/LA	NSIR/CSD/DD*
NAME	FLyon	JBurkhardt	RFelts
DATE	11/18/15	10/22/15	10/5/15
OFFICE	OGC*	NRR/DORL/LPL4-1/BC	NRR/DORL/LPL4-1/PM
NAME	LLondon NLO w/edits	RPascarelli	FLyon
DATE	11/18/15	11/19/15	11/19/15

OFFICIAL RECORD COPY