NEXTera ENERGY
POINT BEACH

[redacted]

July 8, 2010

NRC 2010-0084
10 CFR 50.90

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

Point Beach Nuclear Plant, Units 1 and 2
Dockets 50-266 and 50-301
Renewed License Nos. DPR-24 and DPR-27

License Amendment Request 263A, Request for Approval of the
Point Beach Nuclear Plant Revised Cyber Security Plan

References:
(1) NextEra Energy Point Beach, LLC, letter to NRC, dated November 23, 2009, License Amendment Request 263, Cyber Security Plan (ML093310298)
(2) NextEra Energy Point Beach, LLC, letter to NRC, dated January 18, 2010, License Amendment Request 263, Cyber Security Plan Supplement (ML100190093)
(3) NRC letter to NextEra Energy Point Beach, LLC, dated May 13, 2010, Acceptance Review for Cyber Security Plan Amendment (ML101310209)

In accordance with the provisions of 10 CFR 50.4 and 50.90, NextEra Energy Point Beach, LLC (NextEra) is hereby submitting a request for amendment to the Renewed Facility Operating Licenses for Point Beach Nuclear Plant (PBNP). This proposed amendment requests NRC approval of the NextEra Cyber Security Plan, provides an implementation schedule and revises License Condition D of the Renewed Facility Operating Licenses to require PBNP to fully implement and maintain in effect all provisions of the Commission-approved Cyber Security Plan. The Plan follows NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," with exceptions as described in Enclosure 1.

With this submittal, NextEra withdraws its previous submittals (References 1 and 2) that were based on a prior version of NEI 08-09 guidance.

Enclosure 1 provides an evaluation of the proposed change. Attachment 1 of Enclosure 1 provides the existing Renewed Facility Operating License pages marked up to show the proposed change.

**Enclosure 3 to this letter contains sensitive information.
Withhold from public disclosure under 10 CFR 2.390.
Upon removal of Enclosure 3, this letter is uncontrolled.**

Enclosure 2 provides a copy of the PBNP Cyber Security Plan implementation schedule.

Enclosure 3 provides a copy of the PBNP Cyber Security Plan. The Plan will be incorporated by reference into the NextEra Physical Security Plan upon approval. NextEra requests that Enclosure 3, which contains security-related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

NextEra has evaluated the proposed amendment and has determined that it does not involve a significant hazards consideration pursuant to 10 CFR 50.92. The PBNP Plant Operations Review Committee has reviewed the proposed license amendment request.

NextEra requests an implementation date of December 31, 2013, based upon the enclosed implementation schedule.

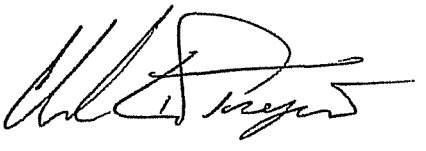
In accordance with 10 CFR 50.91, a copy of this letter is being provided to the designated Wisconsin Official.

If you have any questions or require additional information, please contact James Costedio, Licensing Manager, at 920/755-7427

I declare under penalty of perjury that the foregoing is true and correct.
Executed on July 8, 2010.

Very truly yours,

NextEra Energy Point Beach, LLC



Larry Meyer
Site Vice President

Enclosures

cc: Administrator, Region III, USNRC
Project Manager, Point Beach Nuclear Plant, USNRC
Resident Inspector, Point Beach Nuclear Plant, USNRC
PSCW

**Enclosure 3 to this letter contains sensitive information.
Withhold from public disclosure under 10 CFR 2.390.
Upon removal of Enclosure 3, this letter is uncontrolled.**

ENCLOSURE 1

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

LICENSE AMENDMENT REQUEST 263A
CYBER SECURITY PLAN

EVALUATION OF PROPOSED CHANGE

ATTACHMENT

Attachment 1 - Marked up Renewed Facility Operating License pages

4 pages follow

1.0 SUMMARY DESCRIPTION

The proposed license amendment request (LAR) includes the proposed NextEra Energy Point Beach, LLC (NextEra) Cyber Security Plan for Point Beach Nuclear Plant (PBNP), an implementation schedule and a proposed addition to License Condition D of Renewed Facility Operating Licenses, DPR-24 and DPR-27, for PBNP Units 1 and 2, respectively.

2.0 DETAILED DESCRIPTION

The proposed LAR includes the proposed PBNP Cyber Security Plan, an implementation schedule and a proposed addition to License Condition D of the Renewed Facility Operating Licenses for Units 1 and 2 to require NextEra to fully implement and maintain in effect all provisions of the Commission approved cyber security plan as required by 10 CFR 73.54. *Federal Register* notice 74 FR 13926 (Reference 1) issued the final rule that amended 10 CFR 73. The regulations in 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks, establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under 10 CFR 50 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.

3.0 TECHNICAL EVALUATION

Federal Register notice 74 FR 13926 issued the final rule that amended 10 CFR 73. Cyber security requirements are codified as new 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(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by EA-02-026 (Reference 2).

This LAR includes the proposed change to License Condition D of the Renewed Facility Operating Licenses, Physical Protection (Attachment 1). In addition, the LAR contains the proposed implementation schedule (Enclosure 2) as required by 10 CFR 73.54. Finally, this LAR includes the proposed Plan (Enclosure 3) that conforms to the template provided in NEI 08-09, Revision 6, with the following exceptions:

Definition of Cyber Attack

In lieu of the use of the definition of "cyber attack" in NEI 08-09, Revision 6, the definition of "cyber attack" contained in NEI letter dated June 2, 2010, and as accepted by the Commission via letter dated June 7, 2010, will be used.

Emergency Preparedness

10 CFR 73.54 requires protecting digital computer and communication systems and networks associated with emergency preparedness (EP) functions, including offsite communications. The EP functions within the scope of the Plan are those functions, which support implementation of the Risk Significant Planning Standards* (RSPSs) as defined in NRC Inspection Manual Chapter 0609, Appendix B. The RSPSs are the subset of EP Planning Standards, defined in 10 CFR 50.47(b), which play the greatest role in protecting public health and safety. In terms of

importance, this approach aligns the selected EP functions with other system functions, which are "Safety-Related" or "Important-to-Safety."

10 CFR 73.56(b)(ii) requires that any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's emergency preparedness be subject to an access authorization program. However, some systems, or portions of systems, that perform an RSPS-related EP function may be located in offsite locations not under the control of the licensee and/or not staffed by licensee personnel. Similarly, there may be system components that are normally installed, modified, or maintained by non-licensee personnel (e.g., a telecommunications company technician, employee of a State agency, etc.).

Therefore, the systems, and portions of systems, to be protected from cyber attack in accordance with 10 CFR 73.54(a)(1)(iii) must;

1. Perform a RSPS-related EP function, and
2. Be within the licensee's complete custody and control.

* The RSPSs are 10 CFR 50.47(b)(4), (5), (9), and (10), including the related sections of Appendix E to 10 CFR Part 50. 10 CFR 50.47(b)(10) has two aspects that are of differing risk significance. Only the portion dealing with the development of protective action recommendations (PARs) is integral to protection of public health and safety and is considered to be an RSPS.

Senior Nuclear Management

Senior nuclear management is defined as the Vice President accountable for nuclear plant security. The NEI 08-09 template defines this position as accountable for nuclear plant operations. The position of Vice President accountable for nuclear plant security better reflects the duties and responsibilities of the PBNP Cyber Security Plan.

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

This LAR is submitted pursuant to 10 CFR 73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR 50 to submit a Cyber Security Plan as specified in 10 CFR 50.4 and 10 CFR 50.90.

4.2 Significant Hazards Consideration

NextEra 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 Renewed Facility Operating License to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. Inclusion of the Cyber Security Plan in the Renewed Facility Operating License itself does not involve any modifications to the safety-related structures, systems, or components (SSCs). Rather, the 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 the facility's digital computer and communications systems and networks are protected from cyber attacks. The 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 amendment 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.

   This 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 Renewed Facility Operating License do not result in the need of 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 amendment does not create a possibility for an accident of a new or different type than those previously evaluated.

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

   Response: No.

   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, NextEra 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.

4.3 Conclusions

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 establishes the licensing basis for a Cyber Security Program for NextEra and will be a part of the Physical Security Plan. This proposed amendment will not involve any significant construction impacts. Pursuant to 10 CFR 51.22(c)(12) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

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.

ATTACHMENT 1 TO ENCLOSURE 1

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

LICENSE AMENDMENT REQUEST 263A
CYBER SECURITY PLAN

PROPOSED RENEWED FACILITY
OPERATING LICENSE CHANGES
UNITS 1 AND 2 (MARK-UP)

2 pages follow

D. Physical Protection

NextEra Energy Point Beach 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 combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Point Beach Nuclear Plant Physical Security Plan, (Revision 4)," submitted by letter dated May 10, 2006. NextEra Energy Point Beach, LLC shall fully implement and maintain in effect all provisions of the Commission-approved Point Beach Nuclear Plant cyber security plan submitted by letter dated July 8, 2010, and withheld from public disclosure in accordance with 10 CFR 2.390.

E. Safety Injection Logic

The licensee is authorized to modify the safety injection actuation logic and actuation power supplies and related changes as described in licensee's application for amendment dated April 27, 1979, as supplemented May 7, 1979. In the interim period until the power supply modification has been completed, should any DC powered safety injection actuation channel be in a failed condition for greater than one hour, the unit shall thereafter be shutdown using normal procedures and placed in a block-permissive condition for safety injection actuation.

F. NextEra Energy Point Beach shall implement and maintain in effect all provisions of the approved fire protection program as described in the FSAR for the facility and as approved in the Safety Evaluation Report dated August 2, 1979 (and Supplements dated October 21, 1980, January 22, 1981, and July 27, 1988) and the safety evaluation issued January 8, 1997, for Technical Specification Amendment No. 170, subject to the following provision:

> NextEra Energy Point Beach may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

G. Secondary Water Chemistry Monitoring Program

NextEra Energy Point Beach shall implement a secondary water chemistry monitoring program to inhibit steam generator tube degradation. This program shall include:

1. Identification of a sampling schedule for the critical parameters and control points for these parameters;
2. Identification of the procedures used to quantify parameters that are critical to control points;
3. Identification of process sampling points;
4. Procedure for the recording and management of data;
5. Procedures defining corrective actions for off control point chemistry condition; and

D. Physical Protection

NextEra Energy Point Beach 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 combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Point Beach Nuclear Plant Physical Security Plan, (Revision 4)," submitted by letter dated May 10, 2006. NextEra Energy Point Beach, LLC shall fully implement and maintain in effect all provisions of the Commission-approved Point Beach Nuclear Plant cyber security plan submitted by letter dated July 8, 2010, and withheld from public disclosure in accordance with 10 CFR 2.390.

E. Safety Injection Logic

The licensee is authorized to modify the safety injection actuation logic and actuation power supplies and related changes as described in licensee's application for amendment dated April 27, 1979, as supplemented May 7, 1979. In the interim period until the power supply modification has been completed, should any DC powered safety injection actuation channel be in a failed condition for greater than one hour, the unit shall thereafter be shut down using normal procedures and placed in a block-permissive condition for safety injection actuation.

F. NextEra Energy Point Beach shall implement and maintain in effect all provisions of the approved fire protection program as described in the FSAR for the facility and as approved in the Safety Evaluation Report dated August 2, 1979 (and Supplements dated October 21, 1980, January 22, 1981, and July 27, 1988) and the safety evaluation issued January 8, 1997, for Technical Specifications Amendment No. 174, subject to the following provision:

> NextEra Energy Point Beach may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

G. Secondary Water Chemistry Monitoring Program

NextEra Energy Point Beach shall implement a secondary water chemistry monitoring program to inhibit steam generator tube degradation. This program shall include:

1. Identification of a sampling schedule for the critical parameters and control points for these parameters;
2. Identification of the procedures used to quantify parameters that are critical to control points;
3. Identification of process sampling points;
4. Procedure for the recording and management of data;
5. Procedures defining corrective actions for off control point chemistry condition; and

ENCLOSURE 2

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

LICENSE AMENDMENT REQUEST 263A
CYBER SECURITY PLAN

CYBER SECURITY PLAN IMPLEMENTATION MILESTONE SCHEDULE

4 pages follows

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

CYBER SECURITY PLAN
PROPOSED IMPLEMENTATION SCHEDULE

Generic RAI Question 29 on NEI 08-09, Revision 3, Appendix A, includes reference to previous regulatory guidance and industry initiatives related to cyber security. As referenced, current industry guidance for cyber security is described in NEI 04-04, *Cyber Security Program for Power Reactors*. However, the scope of requirements in the NRC accepted implementation guidance contained in NEI 08-09, Revision 6, are significantly greater than the previously implemented cyber security program. The defensive model design requirements, the new digital asset assessment methodology, and the resultant digital asset remediation actions will require a significant expenditure of labor resources. As referenced in the Generic RAI Question 29, NextEra is also required to implement a separate cyber security program in accordance with the NERC Critical Infrastructure Protection Standards. While the timeframe for implementation is shorter for the NERC regulation, as described in the Generic RAI, the NERC cyber security methodology is different from the NRC Rule requirements. The NERC requirements are based on a logical risk based assessment process while the NRC Rule 73.54 requires a deterministic cyber security assessment methodology.

In light of the extensive work associated with implementation of these two new regulations, NextEra has developed a prioritized approach to establish the NRC Rule 73.54 implementation schedule. NextEra realizes the importance of deploying a uni-directional communication barrier to protect the most critical safety, security, and emergency preparedness (SSEP) functions. One major activity is the deployment of uni-directional communication barrier to ensure protection from remote attacks on plant systems. While the deployment of the uni-directional barrier is critical to protection from external cyber threats, it also impacts remote access to plant data systems by authorized personnel. This elimination of remote access will require Licensees to develop and implement a detailed change management plan.

Another major activity is the performance of individual critical digital asset (CDA) assessments to identify individual asset security control remediation actions. Programs and procedures are being developed to implement the programmatic requirements of the regulation. The cyber security assessment teams are also being established for execution of program requirements. These teams are required to have extensive knowledge of plant systems and cyber security control technology. A comprehensive training program will be required to ensure competent personnel for program execution.

Following are the Cyber Security implementation milestones that have been developed based on the sample listing of milestones provided with the December 2009 implementation schedule guidance.

Implementation Milestone	Completion Date	Basis
Cyber Security Assessment Team (CSAT) identified, trained and qualified.	11/15/2010	The CSAT will require a broad and very specialized knowledge of information and digital systems technology. The CSAT will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team will require additional training in these areas to ensure adequate capabilities to meet the regulation requirements. By the completion date, the following will be performed: • Cyber security assessment procedures/tools will be developed and available; • Qualifications for CSAT will be developed; and • Training of the CSAT will be completed.
Critical System (CS) and Critical Digital Asset (CDA) identification complete	06/15/2011	By the completion date, the following will be performed: • Critical Systems will be identified; and • Critical Digital Assets will be identified.
Develop Cyber Security Defensive Strategy (i.e., defensive model)	02/04/2011	The Defensive Strategy expands upon the high level model in the Cyber Security Plan and requires assessment of existing site and corporate policies, comparison to new requirements, revisions as required, and communication to plant personnel. By the completion date, the following will be performed: • Documenting the defense-in-depth architecture and defensive strategy; • Revisions to existing defensive strategy policies will be implemented and communicated; and • Planning the implementation of the defense-in-depth architecture.
Implementation of Cyber Security defense-in-depth architecture complete	07/01/2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on our plant systems. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers and other plant staff. This elimination of remote access to core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to

Implementation Milestone	Completion Date	Basis
		support the defensive model. The modification will be developed, prioritized, and scheduled. Since software must be updated on and data retrieved from isolated systems, a method of patching, updating, and scanning isolated devices will be developed. By the completion date, the following will be performed: • Installation of one-way diode devices to implement defensive layer boundaries.
Final Cyber Security Assessments as described in the Cyber Security Plan completed and documented.	03/01/2013	Based on the existing cyber security program, it is known that the number of digital assets requiring assessment is extensive. As previously discussed, the CDA assessment methodology required for this regulation is extremely rigorous and deterministic. The completion of these assessments will require a significant commitment of resources. The assessments will not begin prior to having a fully established CSAT and the required procedures. Performing the assessments will require participation of multiple disciplines and involve document reviews, system configuration evaluation, physical walk downs, or electronic verification of every communication pathway for each CDA, and documentation of results. These tasks will need to be coordinated and scheduled to align with department resource availability and system access requirements. By the completion date, the following will be performed: • Cyber security assessments will be performed and documented.
Establish Cyber Security Program policies/procedures.	07/01/2013	The implementation of the cyber security program is expected to require policy/procedure development and/or upgrades for nearly every plant department. The procedural development for the cyber security program requirements and all of the individual security controls will be far-reaching. Many of the security controls will require development of the technical processes for implementing the control in a nuclear plan environment including development of new procedures for surveillances, periodic monitoring, and reviews. Procedure development will begin early in the implementation of the program and continue until the specified completion date. By the completion date, the following will be performed: • Policies/procedures will be updated to establish Cyber

Implementation Milestone	Completion Date	Basis
		Security Program ; • The Cyber Security Assessment Procedure will be issued; and • New policies/procedures or revision of existing policies/procedures in areas impacted by cyber security requirements will be developed and implemented.
Cyber Security Plan Implementation Complete. Implement Security Controls not requiring a plant modification. The Cyber Security Program is implemented and the Program has entered maintenance phase.	12/31/2013	Although the scope of individual CDA assessment remediation actions is unknown, based on the number and complexity of the required security controls, it is expected to be a significant effort. Each of the individual CDA remediation actions will need to be planned, resourced, and executed. This date is only a commitment for the remediation actions not requiring a plant modification. Changes requiring a plant modification may be implemented during the ongoing maintenance of the cyber security program. A rigorous planning process is used to ensure safe execution of refueling outage work. The potential system modifications required by this regulation need to be carefully planned and executed to ensure no detrimental effect to safe plant operations. The Program will be considered implemented and transitioned to the maintenance phase if modifications have either been implemented, or are budgeted and scheduled for implementation. By the completion date, the following will be performed: • Security controls (that do not require plant modification) will be implemented in accordance with Section 3.1.6 of the Plan. The application of security controls requiring plant modifications will be planned, budgeted, and scheduled. Beginning on this date, during the ongoing maintenance of the Program, the following will be included: • The requirements of Section 4 of the Cyber Security Plan will be effective; and • Implementing plant modifications, per the schedule developed above, that have not been completed.

*Commitment changes will be managed in accordance with NEI 99-04, "Guidelines for Managing NRC Commitment Changes."

SECURITY-RELATED INFORMATION
WITHHOLD FROM PUBLIC DISCLOSURE UNDER 10 CFR 2.390

ENCLOSURE 3

NEXTERA ENERGY POINT BEACH, LLC
POINT BEACH NUCLEAR PLANT, UNITS 1 AND 2

LICENSE AMENDMENT REQUEST 263A
CYBER SECURITY PLAN

CYBER SECURITY PLAN

Enclosure 3 to this letter contains sensitive information.
Withhold from public disclosure under 10 CFR 2.390.
Upon removal of Enclosure 3, this letter is uncontrolled.

21 pages follow