

**ENCLOSURES 1 AND 2 TRANSMITTED HEREWITH CONTAIN
SECURITY-RELATED INFORMATION – WITHHOLD UNDER 10 CFR 2.390**

10 CFR 50.90

July 23, 2010

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

Braidwood Station, Units 1 and 2
Facility Operating License Nos. NPF-72 and NPF-77
NRC Docket Nos. STN 50-456 and STN 50-457

Byron Station, Units 1 and 2
Facility Operating License Nos. NPF-37 and NPF-66
NRC Docket Nos. STN 50-454 and STN 50-455

Clinton Power Station, Unit 1
Facility Operating License No. NPF-62
NRC Docket No. 50-461

Dresden Nuclear Power Station, Units 2 and 3
Renewed Facility Operating License Nos. DPR-19 and DPR-25
NRC Docket Nos. 50-237 and 50-249

LaSalle County Station, Units 1 and 2
Facility Operating License Nos. NPF-11 and NPF-18
NRC Docket Nos. 50-373 and 50-374

Limerick Generating Station, Units 1 and 2
Facility Operating License Nos. NPF-39 and NPF-85
NRC Docket Nos. 50-352 and 50-353

Oyster Creek Nuclear Generating Station
Renewed Facility Operating License No. DPR-16
NRC Docket No. 50-219

**Enclosures 1 and 2 transmitted herewith contain Security-Related Information
When separated from Enclosures 1 and 2, this document is decontrolled.**

Peach Bottom Atomic Power Station, Units 2 and 3
Renewed Facility Operating License Nos. DPR-44 and DPR-56
NRC Docket Nos. 50-277 and 50-278

Quad Cities Nuclear Power Station, Units 1 and 2
Renewed Facility Operating License Nos. DPR-29 and DPR-30
NRC Docket Nos. 50-254 and 50-265

Three Mile Island Nuclear Station, Unit 1
Renewed Facility Operating License No. DPR-50
NRC Docket No. 50-289

Subject: Re-submittal of the Exelon Cyber Security Plan

Reference: (1) Letter from Nicholas J. DiFrancesco (U.S. Nuclear Regulatory Commission) to Mr. Charles G. Pardee (Exelon Nuclear), "License Amendment Request for Approval of the Cyber Security Plan," dated June 4, 2010

On November 23, 2009, in accordance with the provisions of 10 CFR 50.4 and 10 CFR 50.90, Exelon Generation Company, LLC (Exelon) submitted a request for an amendment to the Facility Operating Licenses (FOL) for Braidwood Station, Units 1 and 2; Byron Station, Units 1 and 2; Clinton Power Station, Unit 1; Dresden Nuclear Power Station, Units 2 and 3; LaSalle County Station, Units 1 and 2; Limerick Generating Station, Units 1 and 2; Oyster Creek Nuclear Generating Station; Peach Bottom Atomic Power Station, Units 2 and 3; Quad Cities Nuclear Power Station, Units 1 and 2; and Three Mile Island Nuclear Station, Unit 1. This proposed amendment requested U.S. Nuclear Regulatory Commission (NRC) approval of the Exelon Cyber Security Plan, provided an Implementation Schedule, and added a sentence to the existing FOL Physical Protection license condition to require Exelon to fully implement and maintain in effect all provisions of the Commission-approved Cyber Security Plan. This proposed amendment conformed to the model application contained in NEI 08-09, Revision 3, submitted to the NRC for endorsement on September 15, 2009. This amendment request was supplemented on January 15, 2010, with a revised No Significant Hazards Consideration (NSHC) Determination.

By letter dated April 28, 2010, NEI submitted to the NRC, Revision 6 to NEI 08-09, which contains changes that address NRC staff concerns associated with previous versions. Based on a technical review of the document, the Office of Nuclear Security and Incident Response, in its letter dated May 5, 2010, concluded that submission of a cyber security plan using the template provided in NEI 08-09, Revision 6, dated April 2010, would be acceptable for use by licensees to comply with the requirements of 10 CFR 73.54, with the exception of the definition of "Cyber Attack." A revised definition for Cyber Attack to be utilized in the Exelon Cyber Security Program is provided in the attached Evaluation of NEI 08-09, Revision 6 Deviations.

Therefore, to resolve the NRC staff's concerns with Revision 3 to NEI 08-09 and with the NEI 08-09, Revision 6 definition of "Cyber Attack," Exelon is providing a revised Cyber Security Plan consistent with NEI 08-09, Revision 6 for Braidwood Station, Units 1 and 2; Byron Station, Units 1 and 2; Clinton Power Station, Unit 1; Dresden Nuclear Power Station, Units 2 and 3; LaSalle

County Station, Units 1 and 2; Limerick Generating Station, Units 1 and 2; Oyster Creek Nuclear Generating Station; Peach Bottom Atomic Power Station Units 2 and 3; Quad Cities Nuclear Power Station, Units 1 and 2; and Three Mile Island Nuclear Station, Unit 1. The attached Cyber Security Plan, Implementation Schedule/Summary of Regulatory Commitments and Evaluation of Deviations supersede, in its entirety, the previous Cyber Security Plan, Implementation Schedule/Summary of Regulatory Commitments and Evaluation of Deviations submitted on November 23, 2009.

Enclosure 1 provides a copy of the Exelon Cyber Security Plan which supersedes in its entirety the November 23, 2009, Cyber Security Plan. This is a standalone document that will be incorporated by reference into the Exelon Physical Security Plan upon approval. Enclosure 2 provides a response to NRC's generic question #29 provided to NEI regarding NEI 08-09, Revision 3, and Implementation Schedule/Summary of Regulatory Commitments. This question was not directly addressed on an industry level and is therefore provided as part of this supplement. Enclosure 3 provides an evaluation of deviations from NEI 08-09, Revision 6. Exelon requests that Enclosures 1 and 2, which contain sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390.

In accordance with 10 CFR 50.91, a copy of this application with attachments is being provided to the designated State Officials. If you should have any questions regarding this submittal, please contact Mr. Doug Walker at 610-765-5952.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the 23rd day of July 2010.

Respectfully,

Pamela B. Cowan

Pamela B. Cowan
Director - Licensing and Regulatory Affairs

Enclosure 1 - Cyber Security Plan For Exelon Nuclear
Enclosure 2 - Evaluation of NRC's Generic Question #29 on NEI 08-09, Revision 3 and
Implementation Schedule/Summary of Regulatory Commitments
Enclosure 3 - Evaluation of NEI 08-09, Revision 6 Deviations

cc: USNRC Region I, Regional Administrator
USNRC Region III, Regional Administrator
NRC Project Manager, NRR - Braidwood Station
NRC Project Manager, NRR - Byron Station
NRC Project Manager, NRR - Clinton Power Station
NRC Project Manager, NRR - Dresden Nuclear Power Station
NRC Project Manager, NRR - LaSalle County Station
NRC Project Manager, NRR - Limerick Generating Station
NRC Project Manager, NRR - Oyster Creek Nuclear Generating Station
NRC Project Manager, NRR - Peach Bottom Atomic Power Station
NRC Project Manager, NRR - Quad Cities Nuclear Power Station
NRC Project Manager, NRR - Three Mile Island Nuclear Station

cc-continued

USNRC Senior Resident Inspector - Braidwood Station

USNRC Senior Resident Inspector - Byron Station

USNRC Senior Resident Inspector - Clinton Power Station

USNRC Senior Resident Inspector - Dresden Nuclear Power Station

USNRC Senior Resident Inspector - LaSalle County Station

USNRC Senior Resident Inspector - Limerick Generating Station

USNRC Senior Resident Inspector - Oyster Creek Nuclear Generating Station

USNRC Senior Resident Inspector - Peach Bottom Atomic Power Station

USNRC Senior Resident Inspector - Quad Cities Nuclear Power Station

USNRC Senior Resident Inspector -Three Mile Island Nuclear Station

S. T. Gray, State of Maryland

Illinois Emergency Management Agency - Division of Nuclear Safety

R. R. Janati - Bureau of Radiation Protection, Commonwealth of Pennsylvania

ENCLOSURE 3

**Evaluation of NEI 08-09, Revision 6
Deviations**

#	NEI 08-09 Location	NEI 08-09 Rev 6 Text	Exelon Text	Discussion
1	Appendix A, Section 3.1.2, 6th bullet, last phrase	<p>The roles and responsibilities of the CSAT include such activities as:</p> <ul style="list-style-type: none"> Evaluating assumptions and conclusions about cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs and cyber security controls throughout their system life cycles; and estimates of cyber security risk 	<p>The roles and responsibilities of the CSAT include such activities as:</p> <ul style="list-style-type: none"> Evaluating assumptions and conclusions about cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs and cyber security controls throughout their system life cycles; and estimates of cyber security risk 	<p>This deviation deletes the CSAT responsibility for estimating cyber security risk since there is no basis for performing this action (e.g., how to perform this function, when this is performed, or how the information is used). This bullet has been revised and now reads consistent with Reg Guide 5.71.</p>
2	Appendix A, Section 3.1.4, first paragraph	<p>The CSAT collects, examines, and documents the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process. The team collects, documents by reference and evaluates the following as they apply to CDAs</p>	<p>The CSAT collects, examines, and documents the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process. The team collects, documents by reference and evaluates examines the following as they apply to CDAs</p>	<p>The word “evaluates” has been replaced by “examines” to be consistent with both the Title of the section and other uses of the word in the section. It is clear that there is no additional evaluation implied with this requirement and the text should be revised to read “examine” to avoid unintended meaning.</p>

#	NEI 08-09 Location	NEI 08-09 Rev 6 Text	Exelon Text	Discussion
3	Appendix A, Section 4.4.3.2, last paragraph, first sentence	A vulnerability assessment may be used as a substitute for vulnerability scanning where there is a risk of an adverse impact to SSEP functions, and when off-line, replicated, or vendor test beds are not available.	A vulnerability assessment may be used as a substitute for vulnerability scanning where there is a risk of an adverse impact to SSEP functions, and when off-line, replicated, or vendor test beds are not available or when a scan is technically inappropriate to be performed.	There are many CDAs that operate as single-function, isolated instruments. It is technically inappropriate to scan isolated instruments such as transmitters, recorders, indicators, controllers, and programmable logic controllers (PLCs). Vulnerability scans on these instruments will not provide valid/usable results.
4	Appendix A Section 4.7	<ul style="list-style-type: none"> Procedures for operating the CDAs in manual mode with external electronic communications connections severed until secure conditions can be restored 	<ul style="list-style-type: none"> Procedures for severing external electronic communications connections, where allowed operating the CDAs in manual mode with external electronic communications connections severed, until secure conditions can be restored 	Deleted "operating the CDAs in manual mode" based on its conflict with the Technical Specification Limiting Conditions for Operation as defined under 10 CFR 50.36. There may be conditions and CDAs in a nuclear power plant that are not permitted to be operated in manual mode with external communication connections severed. This deviation revises the requirement to sever the communication connections where allowed and deletes the requirement to operate the CDA in a manual mode.
5	Appendix B, definition of Cyber Attack	Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a SSEP function.	Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a SSEP function CDA.	This revision to the definition of Cyber Attack results from comments provided by NRC following their review of NEI 08-09, Rev 6. Reference letter from NEI Christopher E. Earls to NRC Richard P. Correia dated June 2, 2010.

#	NEI 08-09 Location	NEI 08-09 Rev 6 Text	Exelon Text	Discussion
6	Appendix D, Control 1.4, 6 th and 7 th bullets	<p>1.4 Information Flow Enforcement This Technical cyber security control:</p> <ul style="list-style-type: none"> • Implements one-way data flows using hardware mechanisms, implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations. • Implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions. 	<p>1.4 Information Flow Enforcement This Technical cyber security control:</p> <ul style="list-style-type: none"> • For Deterministic devices: Implements one-way data flows using hardware mechanisms, implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations. • For Non-deterministic devices: Implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions. 	<p>The two bulleted controls here are being revised to remove ambiguity in how they are applied to both non-deterministic firewalls and deterministic data diodes. Both types of devices are being implemented as part of Exelon's defensive architecture.</p>
7	Appendix D, Control 2.5, 4 th bullet, 3 rd sub-bullet	<p>o Ensures CDAs with auditing failures take the following additional actions:</p> <ol style="list-style-type: none"> 1. Shut down the CDA, 2. Failover to a redundant CDA, where necessary to prevent adverse impact to safety, security or emergency preparedness functions, 3. Overwrite, when necessary, the oldest audit record(s), and 4. Stop generating audit records. 	<p>o Ensures CDAs with auditing failures take the following additional actions:</p> <ol style="list-style-type: none"> 1. Shut down the CDA (if appropriate), 2. Failover to a redundant CDA, where necessary to prevent adverse impact to safety, security or emergency preparedness functions, 3. Overwrite, when necessary, the oldest audit record(s), and 4. Stop generating audit records. 	<p>Appendix D, Control 2.5 discusses "Response To Audit Processing Failures." The Control states that CDAs should be shut down when auditing failures occur. Depending on the function of the CDA in a nuclear power plant, it may not be possible in all circumstances to shut down a CDA. The control is being revised to acknowledge the CDA may not be able to be immediately shut down.</p>

#	NEI 08-09 Location	NEI 08-09 Rev 6 Text	Exelon Text	Discussion
8	Appendix E, Section 6, 4 th bullet and next to last sub-bullet.	<p>This security control implements and documents a defensive strategy that:</p> <ul style="list-style-type: none"> • Allows only one-way direct data flow from higher security levels to lower security levels. <p>In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:</p> <ul style="list-style-type: none"> ○ Except in the case of data diodes, contain a rule set that at a minimum <ul style="list-style-type: none"> ▪ Allows no information of any kind, including handshaking protocols, to be transferred directly from networks or systems existing at the lower security level to networks or systems existing at the higher security level; 	<p>This security control implements and documents a defensive strategy that:</p> <ul style="list-style-type: none"> • For deterministic devices (e.g., data diodes), allows only one-way direct data flow from higher security levels to lower security levels. <p>In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:</p> <ul style="list-style-type: none"> ○ Except in the case of data diodes, contain a rule set that at a minimum <ul style="list-style-type: none"> ▪ Allows no information of any kind, including handshaking protocols, to be transferred directly from networks or systems existing at the lower security level to networks or systems existing at the higher security level; 	<p>For Exelon, the boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above level 3. The boundary between level 4 and level 3 is implemented by either one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in level 4, or one or more non-deterministic network isolation devices. Information flows between level 3 and 4 are restricted through the use of a firewall and network-based intrusion detection system.</p> <p>The first revised bullet discusses the restriction to one-way communication between levels. Exelon's defensive architecture allows use of a firewall within the boundary of a deterministic device (i.e., level 3 to level 4) which under controlled conditions may allow some transfer of information from lower to higher level.</p> <p>The second revised bullet is deleted. This bullet discusses boundary devices other than diodes (e.g., firewalls). The restriction of no data transfer is removed and not necessary in Exelon's architecture which employs a data diode or air gap between level 2 and level 3.</p>

#	NEI 08-09 Location	NEI 08-09 Rev 6 Text	Exelon Text	Discussion
9	Appendix E Control 7.1, last paragraph	<p>Stakeholders are included in the development of incident response policies, procedures and plans, including the following groups:</p> <ul style="list-style-type: none"> • Physical security • Cyber security team • Operations • Engineering • Information Technology • Human resources • System support vendors • Management • Legal • Safety 	<p>Stakeholders are included in the development of incident response policies, procedures and plans. including the following groups For example:</p> <ul style="list-style-type: none"> • Physical security • Cyber security team • Operations • Engineering • Information Technology • Human resources • System support vendors • Management • Legal • Safety 	<p>Appendix E, Control 7.1 is revised to recognize that all groups listed in the control are provided for example and not necessarily all required for the development of the incident response policies, procedures and plans.</p>