



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

January 5, 2011

Vice President, Operations
Entergy Nuclear Operations, Inc.
Indian Point Energy Center
450 Broadway, GSB
P.O. Box 249
Buchanan, NY 10511-0249

SUBJECT: INDIAN POINT NUCLEAR GENERATING UNIT NOS. 1, 2 AND 3 - REQUEST FOR ADDITIONAL INFORMATION REGARDING AMENDMENT APPLICATION FOR APPROVAL OF THE INDIAN POINT CYBER SECURITY PLAN (TAC NOS. ME4212, ME4213, AND ME4214)

Dear Sir or Madam:

By letter dated July 8, 2010 (Agencywide Documents Access and Management System Accession No. ML101970048), Entergy Nuclear Operations, Inc. (the licensee) resubmitted a request to amend the Facility Operating Licenses (Nos. DPR-5, DPR-26, and DPR-64) for Indian Point Generating Unit Nos. 1, 2, and 3 (IP1, IP2, and IP3). Per the proposed license amendment, the licensee requested approval of the IP1, IP2 and IP3 Cyber Security Plan (CSP), provided a proposed CSP Implementation Schedule, and included a proposed revision to the Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved CSP. The licensee's amendment request was based on a generic template developed by the Nuclear Energy Institute in concert with the industry.

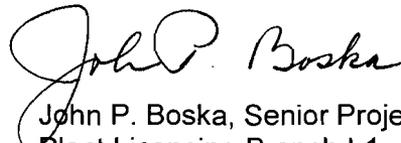
The Nuclear Regulatory Commission (NRC) staff is reviewing the CSP and the proposed CSP Implementation Schedule and has determined that additional information is required to complete its technical review. The specific questions are found in the enclosed request for additional information (RAI). On January 4, 2011, the Entergy staff indicated that a response to the RAI would be provided within 45 days of the date of this letter.

V. P. Operations

-2-

Please contact me at (301) 415-2901 if you have any questions on this issue.

Sincerely,

A handwritten signature in black ink that reads "John P. Boska". The signature is written in a cursive style with a large initial "J" and "B".

John P. Boska, Senior Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-003, 50-247, and 50-286

Enclosure:
RAI

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION
REGARDING APPROVAL OF THE CYBER SECURITY PLAN
ENERGY NUCLEAR OPERATIONS, INC.
INDIAN POINT NUCLEAR GENERATING UNIT NOS. 1, 2, AND 3
DOCKET NOS. 50-003, 50-247, AND 50-286

Cyber Security Plan (CSP) Section 4: Establishing, Implementing, and Maintaining the Cyber Security Program

RAI 1:

RAI Title: Defense-in-Depth Protective Strategies – Critical Digital Asset (CDA) Isolation Strategies

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. CSP Section 4.3, "Defense-in-Depth Protective Strategies," of the Indian Point CSP states in several instances when referring to protections which isolate or secure CDAs within various cyber security defensive levels, that boundaries may be secured via "an air gap or deterministic one-way isolation device such as a data diode or hardware VPN [virtual private network]."

Please clarify how hardware VPNs will sufficiently protect CDAs within defensive boundaries, including an explanation of the technical configurations that would enable it to mimic the capabilities of a deterministic one-way isolation device.

RAI 2:

RAI Title: Defense-in-Depth Protective Strategies – Protection of CDAs Associated with Emergency Preparedness Functions

Section 73.54(a)(1) of 10 CFR requires that "The licensee shall protect digital computer and communication systems and networks associated with... (iii) Emergency preparedness functions, including offsite communications; and (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions."

CSP Section 4.3, "Defense in Depth Protective Strategies," in describing its site defensive model, states that CDAs that "are not required to be within Level 4 due to their safety or security significance, and that perform security or Emergency Plan functions and security or Emergency Plan data acquisition or that perform safety monitoring, are within Level 3." Furthermore, the CSP states that "CDAs that are not required to be in at least Level 3 and that perform or support Emergency Plan functions are within Level 2."

Enclosure

The CSP does not indicate which protective strategies will be implemented for CDAs that perform Emergency Preparedness functions. Please clarify (1) the distinction between CDAs that perform Emergency Planning and Emergency Preparedness functions; and (2) which protective strategies will be implemented for CDAs that perform “emergency preparedness” functions.

RAI 3:

RAI Title: Roles and Responsibilities – Cyber Security Incident Response Team (CSIRT)

Sections 73.54(c)(1) – (4) of 10 CFR, requires the licensee to implement a cyber security program that: (a) protects the assets identified by 10 CFR 73.54(b)(1) from cyber attacks; (b) applies and maintains defense-in-depth protective strategies to ensure the capability to detect, respond to and recover from cyber attacks; (c) mitigate the adverse affects of cyber attacks; and (d) ensure that the functions of protected assets identified by 10 CFR 73.54(b)(1), are not adversely impacted due to cyber attacks. CSP Section 4.11, describing the Roles and Responsibilities of the Cyber Security Incident Response Team (CSIRT), states that the CSIRT “responds to a *credible* cyber attack and performs the activities described in Section 4.6” (of the Indian Point CSP).

Please explain the approach the Indian Point CSIRT will take to determine the “credibility” of a cyber attack.

V. P. Operations

-2-

Please contact me at (301) 415-2901 if you have any questions on this issue.

Sincerely,

/ra/

John P. Boska, Senior Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-003, 50-247, and 50-286

Enclosure:

RAI

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNrrDorlLpl1-1	RidsNrrPMIndianPoint	RidsOGCRp
LPL1-1 Reading File	RidsNrrLASLittle	RidsAcrsAcnw_MailCTR	
RidsNrrDorlDpr	RidsRgn1MailCenter	RidsNsirlscpb	CErlanger, NSIR/ISCPB

ADAMS ACCESSION NO.: ML103560031 (*) See memo dated 12/14/10 **Concur via email

OFFICE	LPL1-1/PM	LPL1-1/LA**	NSIR/ISCPB/BC*	LPL1-1/BC	LPL1-1/PM
NAME	JBoska	SLittle	CErlanger	NSalgado	JBoska
DATE	1/5/11	12/29/10	12/14/10	1/5/11	1/5/11

OFFICIAL RECORD COPY