State of Florida

Public Service Commission

CAPITAL CIRCLE OFFICE CENTER • 2540 SHUMARD OAK BOULEVARD
TALLAHASSEE, FLORIDA 32399-0850

-M-E-M-O-R-A-N-D-U-M-

DATE:	April 16, 2008
TO:	Ann Cole, Commission Clerk - PSC, Office of Commission Clerk
FROM:	Rosanne Gervasi, Senior Attorney, Office of the General Counsel
RE:	Docket No. 080061-EI - Revised Redacted 3.18.08

Please file the attached amended redacted pages in the above docket file.

RG
Attachment

RECEIVED-FPSC
08 APR 16 PM 1:29
COMMISSION
CLERK

CMP _____
COM _____
CTR _____
ECR _____
GCL _____
OPC _____
RCA _____
SCR _____
SGA _____
SEC _____
OTH Marguerite

DOCUMENT NUMBER-DATE
02979 APR 16 08
FPSC-COMMISSION CLERK

Rosanne Gervasi

From: Stright, Lisa [Lisa.Stright@pgnmail.com]
Sent: Tuesday, March 18, 2008 5:20 PM
To: Rosanne Gervasi
Cc: Burnett, John
Subject: Request for CC - Data Security Audit
Attachments: Revised Redacted 3.18.08.pdf

Roseanne:

I have reviewed the Request for CC and Confidential Exhibit A - Page 54 (lines 25-26) and Page 57 (lines 2-5) which PEF originally claimed as confidential. Upon further review, it has been determined that the lines cited above are NOT confidential. I have attached revised redacted versions of Page 54 and 57.

<<Revised Redacted 3.18.08.pdf>>

Please let me know if there is anything else you need.

Lisa Stright
Regulatory Analyst - Legal Dept.
Progress Energy
106 E. College Ave., Suite 800
Tallahassee, FL 32301
(850) 222-8738 office
(850) 222-9768 fax
Email: lisa.stright@pgnmail.com

Does Progress Energy Florida adequately limit the use and disclosure of customers' personal information?

Progress Energy Florida's CSS system maintains its customer account and billing records. [redacted] Each PEF associate is assigned unique log on identification. Access to the network systems is assigned to users' identification based on job classification. Each associate must create a unique password, which must be updated every 60 days.

[redacted]

[redacted]

[redacted]

When processing customer payments, the company incorporates components of the Sarbanes-Oxley act within its procedures. [redacted]

PEF collects images of each payment during its remittance process. These images are stored on CDs for future use, and a vendor software package is needed to access these images. [redacted]

network facilities are also monitored via logs. The payment processing unit [redacted] also requires key-card access and is limited to the associates assigned to this unit.

Does Progress Energy Florida restrict access to customer information software-related functions, data, and programs?

PEF information security area continually monitors and evaluates the network for unauthorized access. The company's approach to securing customer information is to assign user rights based on job function. The company goal is to limit the number of associates who have access to sensitive information to the least number possible. The company states that one area where it has recently accomplished this goal is reducing the number of associates with access to full social security numbers.

The company has a series of reviews that monitor an associate's user rights and system access rights. The company has a policy, the *Critical Application Access Review Processes Policy*, which outlines the required monitoring of system access. Examples of reviews conducted by the management include the monitoring of the transfer and termination of employees each pay period and a report that lists all associates with restricted access.

Progress Energy's IT division is involved in each of the company's change management processes that impact the network. The company has a set of standards, *Application Security Standards and Guidelines*, which outline how the company implements and makes changes to its production applications.

Does Progress Energy Florida monitor software security activity and produce appropriate management reports?

Progress Energy continually monitors its software and network activities to deter and prevent unauthorized access to the system. The company has specific procedures that address Resource Monitoring. The IT security analyst monitors and reports any unauthorized activity to IT management.

The company also has implemented a series of management controls to monitor access to customer information. The company routinely verifies its user log-in identification access. Access to information is controlled by job level and user access. Every six months, management reviews an IT listing of all employees with restricted access. This allows management to verify that an associate's access is still necessary based on their current job responsibilities.