080062-EI

# EXHIBIT B

CMP 1
COM
CTR
ECR
GCL
OPC
RCA
SCR
SGA
SEC
OTH

DOCUMENT NUMBER-DATE
10947 DEC 14 05
FPSC-COMMISSION CLERK

COMMISSIONERS:
LISA POLAK EDGAR, CHAIRMAN
MATTHEW M. CARTER II
KATRINA J. MCMURRIAN
NANCY ARGENZIANO
NATHAN A. SKOP

**STATE OF FLORIDA**

DIVISION OF COMPETITIVE MARKETS & ENFORCEMENT
BETH W. SALAK
DIRECTOR
(850) 413-6600

# Public Service Commission

November 16, 2007

Mr. Bill Feaster
Manager, Regulatory Affairs
Florida Power & Light Company
215 South Monroe Street, Suite 810
Tallahassee, Florida 32301-1859

Dear Mr. Feaster:

Enclosed is a draft copy of our report entitled ***Customer Data Security of Florida's Five Investor-Owned Utilities.*** This draft includes the Executive Summary, Background & Perspective, the Florida Power & Light Company chapter, and three appendices. The review examined the data security practices for each of Florida's five-investor owned utilities. It is our hope that each company finds this assessment beneficial.

This draft is provided for review of factual accuracy and identification of any material on which you intend to file a request for confidential classification. You have the right to file a request in accordance with *Rule 25-22.006(3), F.A.C.* The request must be filed with the Division of the Commission Clerk and Administrative Services no later than 21 days from the date of receipt, or we retain the right to publish without regard to confidentiality. During the next 21 days, staff will be available to discuss the factual accuracy of the report and to provide access to work papers for review of prospective confidential information. Also during this period, staff will accept any written comments the company may want to include in the final report.

We would like to publish the report as soon as possible after the 21 day period for filing expires on **December 11, 2006.** Thank you for your cooperation and assistance, and that extended by Florida Power & Light Company employees who participated in this review. If you have any questions, please contact **David Rich** at (850) 413-6830.

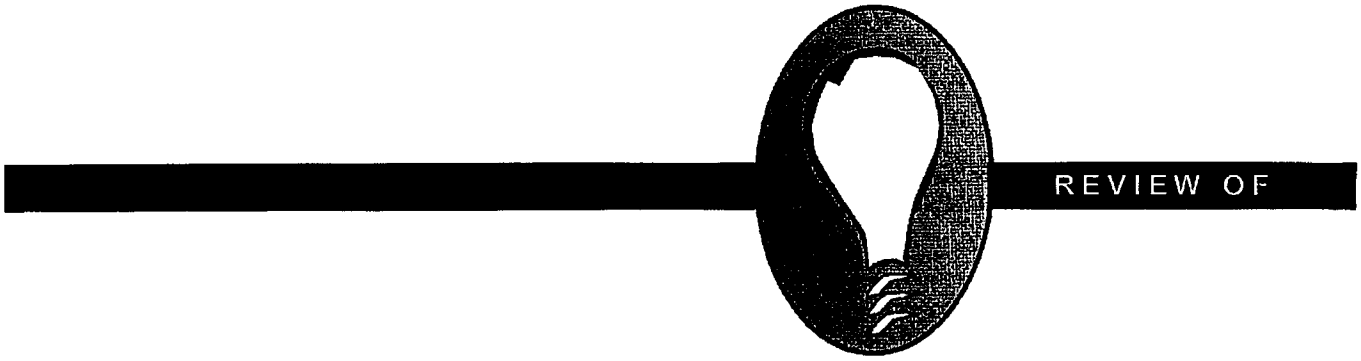
Sincerely,

Lisa S. Harvey
Bureau Chief

cc: Beth Salak, Director, Division of Competitive Markets and Enforcement
Dale Mailhot, Assistant Director, Division of Competitive Markets and Enforcement

FPL

NOVEMBER 2007




# Customer Data Security

OF

# Florida's Five Investor-Owned Electric Utilities

By Authority of
The State of Florida
Public Service Commission
Division of Competitive Markets and Enforcement
Bureau of Performance Analysis

*Review of*

# Customer Data Security of Florida's Five Investor-Owned Electric Utilities


**William "Tripp" Coston**
**Project Manager,**
**Operations Review Specialist**

**David F. Rich**
**Operations Review Specialist**


**November 2007**


**By Authority of**
**The State of Florida for**
**The Public Service Commission**
**Division of Competitive Markets and Enforcement**
**Bureau of Performance Analysis**

**PA-07-05-005**

# TABLE OF CONTENTS

# 1.0 Executive Summary

## 1.1 Objectives

This review of Florida's investor-owned electric utilities was conducted on behalf of the Florida Public Service Commission (the Commission) by the Bureau of Performance Analysis. The objective of the review was to learn more about each company's policies, practices, and controls regarding the security of sensitive customer information.

The primary objectives of this review were:

- To become familiar with, document, and evaluate each investor-owned utility's policies, practices, and procedures for safeguarding sensitive customer data,
- To determine whether sufficient physical and virtual internal controls exist in each utility to protect customer sensitive data and the network, and
- To ensure that each company is in compliance with applicable state, federal, and industry guidelines regarding protection of sensitive customer data.

## 1.2 Scope

The review focused on examining each company's procedures, processes, network systems, and operational controls for safeguarding sensitive customer data. Staff reviewed information technology (IT) security and customer account security in each company. Internal and external audits associated with IT and data security, from 2005 to the present, were also reviewed.

Specifically, staff focused its review on the following functional areas:

- Management Oversight,
- Information Technology Controls,
- User Awareness,
- Outsourcing Controls, and
- Audits of Data Security.

## 1.3 Methodology

The five investor-owned utilities were each reviewed separately. During the review, staff gathered information from each company through document requests. After careful study of the responses from the document requests, staff conducted on-site interviews with each company. Key company employees in the functional areas were interviewed. The review was conducted between June and October 2007.

Each company's policies, practices, and procedures were compared to applicable state and federal statutes relevant to the protection of sensitive customer data. Staff made comparisons to relevant standards such as those shown in **APPENDIX A.** Staff also reviewed the current physical and virtual security systems used by each company, those now being implemented, and concepts in stages of either planning or development.

To assess and compare companies' overall security posture, staff used the information gathered from the document reviews, on-site interviews, and facility visits to assess each company's overall security status.

## 1.4 Overall Opinion

All of the companies are in compliance with applicable state and federal statutes and industry guidelines for security of sensitive customer information.

Each company recognizes the integral role management has in establishing an overall corporate climate conducive to safeguarding customer information. Management in each investor-owned utility has tailored company goals and objectives, policies, programs, and procedures to respond to their particular information security environment and perceived risk.

No company reported, or is aware of, any breaches to sensitive customer information in the previous two years, the period covered by this review. However, each company is variously impacted by the accelerated pace of evolving technology and continued vigilance is required.

**EXHIBIT 1** presents a summary of the Data Security issues observed during staff's review. Where staff found each category of controls to be appropriate and adequate, this is indicated in the chart by a solid circle (●) symbol. Where a deficiency was noted, this is indicated in the chart by an open circle (○) symbol. The Control Elements within Management Oversight, IT Controls, User Awareness, Outsourcing Controls, and Auditing Controls are individually discussed in more detail in chapters three through seven.

# Customer Data Security Issue Summary

| MANAGEMENT OVERSIGHT | | | | | |
|---|---|---|---|---|---|
| CONTROL ELEMENTS | FPL | FPU | GULF | PROGRESS | TEC |
| Clearly understands that information security is a management responsibility | | | | | |
| Personal information is collected | | | | | |
| Assesses the appropriateness of the information collected from customers | | | | | |
| Adequately limits the use and disclosure of customer's personal information | | | | | |
| Access to customer information from remote locations | | | | | |
| Controls for remote access to customer information | | | | | |

| IT CONTROLS | | | | | |
|---|---|---|---|---|---|
| | FPL | FPU | GULF | PROGRESS | TEC |
| Appropriate data security management function exists | | | | | |
| Appropriate information security policies and procedures exist | | | | | |
| Access to customer data is physically limited | | | | | |
| Access to software, data, and functions are restricted | | | | | |
| Management routinely monitors and assesses system security | | | | | |

| USER AWARENESS | | | | | |
|---|---|---|---|---|---|
| | FPL | FPU | GULF | PROGRESS | TEC |
| Adequate privacy and data security policy and procedures exist | | | | | |
| Proper training on privacy and data security policies is provided | | | | | |
| Penalties for violations of privacy or data security policies are documented | | | | | |

| OUTSOURCING CONTROLS | | | | | |
|---|---|---|---|---|---|
| | FPL | FPU | GULF | PROGRESS | TEC |
| Access to customer information provided to third parties | | | | | |
| Controls are in place to prevent disclosure of customer information by third parties | | | | | |

| AUDITING CONTROLS | | | | | |
|---|---|---|---|---|---|
| | FPL | FPU | GULF | PROGRESS | TEC |
| Access to competent data security auditing resources exist | | | | | |
| Data security is periodically assessed | | | | | |
| Information security breaches are reported to appropriate management | | | | | |

● No Issue ○ Issue

EXHIBIT 1

*Source: Company Data requests 1 and 2*

Staff's findings for each company are summarized below. Additional discussion of staff's conclusions for each company is contained in chapters three through seven. A profile of company data security information is provided in **APPENDIX B.** A company-by-company recap of the treatment of sensitive customer data is provided in **APPENDIX C.**

### 1.4.1 Florida Power & Light (FP&L)

Overall, staff found that FP&L has an effective data security program. Company operations and controls appear to adequately protect sensitive customer information. Generally, sufficient physical and virtual controls are in place to protect both customers' information and the company network. Additionally, staff believes that FP&L is in compliance with applicable state, federal, and industry guidelines regarding the protection of sensitive customer information.

However, staff has concerns about certain areas of FP&L's efforts to protect sensitive customer information. The most concerning issues center around the following practices or procedures:

- [redacted]
- [redacted]
- [redacted]

### 1.4.2 Florida Public Utilities Company (FPU)

CONFIDENTIAL

### 1.4.3 Gulf Power Company (Gulf Power)

### 1.4.4 Progress Energy Florida (PEF)

### 1.4.5 Tampa Electric Company (TEC)

# 2.0 Background and Perspective

The social security number is one of the most valuable bits of information needed to commit identity fraud. The social security number has evolved from a tracking number used by the government's retirement system to a personal identification number used by such entities as the Internal Revenue Service and Credit Reporting Agencies. This evolution of the social security number has created a greater need to protect and secure its use and exposure. While the social security number is the most critical component for identity theft, other information such as date of birth, driver's license number, address, phone number, and credit card account numbers can also be useful in facilitating identity theft.

Each individual bears the responsibility to be judicious in securing his personal information. Many times, identity theft occurs when a victim loses his information or carelessly exposes the information to opportunistic thieves. However, there are times when consumers must entrust personal information to a business or agency. Therefore, there is an expectation that reputable companies, such as utilities and financial institutions, will earnestly protect this sensitive information.

## 2.1 Federal Trade Commission Role

In 1998, the Federal government enacted the Identity Theft and Assumption Deterrence Act which made it a violation of federal law to intentionally misuse someone's identifying information or existing accounts, or to establish an account in his name.[1] The act charged the Federal Trade Commission (FTC) as the federal governmental agency that works to protect consumers from identity theft. Citizens who are victims of identity theft can report the crime to the FTC, and the FTC is charged with collecting complaints from victims and sharing the information with necessary federal, state, and local law enforcement.

In 2003, the FTC sponsored a survey on the topic of identity theft. The results support the concerns of many Floridians: identity theft is a real threat; protecting one's personal information is critical. In general terms, identity theft is the use of someone's personal information with the intent to commit fraud. Identity theft can include the establishment of a new account without authorization, the misuse of an existing account, and the establishment or misuse of government documents and benefits.

The *2003 FTC Identity Theft Survey Report* indicated that during the previous 12 months, 4.6 percent of the population experienced some type of identity theft. In the previous five years, 12.7 percent (approximately 27 million citizens) reported being victims of some type of identity theft. The report shows that identity theft impacted 9.91 million citizens in the previous 12 months at a cost of $52.6 billion. The report also states that, on average, it takes a victim 30 hours of work to resolve the impacts of identity theft; with up to 60 hours expended in situations where a new account is fraudulently established.[2]

[1] Public Law 105-318,112 Stat.3007 (October 30,1998)
[2] *2003 FTC Identity Theft Survey Report*

The FTC tracks complaints annually by type and location. In 2006, Florida ranked fifth in the nation (cases per 100,000), with 17,780 reported victims. The Miami-Fort Lauderdale Metropolitan Statistical Area had the largest number of Florida complainants in 2006, at 7,557.[3] The total number of reported victims within the state has increased each year, with 12,816 in 2002; 14,119 in 2003; 16,062 in 2004; and 17,048 in 2005.[4] These numbers only represent the number of victims who notified the FTC of the crime, rather than the actual total number of victims during the period. The 2003 FTC study notes that only 25 percent of the participants reported the crime to local police, and only 22 percent notified a credit agency.[5]

The FTC categorizes complaints based on how the victims' information was misused, including phone or utility fraud. Of note, the 2006 Florida data indicates that approximately 4.7 percent of complainants reported unauthorized establishment of new (non-telecommunications) utility accounts. This has increased from a low of 3.3 percent in 2003.[6]

## 2.2 Data Security Breaches

One of the most publicized breaches occurred in 2005, when consumer data broker, ChoicePoint, Inc., admitted that it had compromised 163,000 consumers in its database. The company sold personal information, such as names, social security numbers, birth dates, employment information, and credit histories to an international group posing as legitimate American businessmen. The individuals lied about their credentials and used commercial domestic mail drops as their business address. ChoicePoint not only ignored red flags, but used unsecured fax machines for correspondences. [7]

Also in 2005, Bank of America admitted to losing a back-up file that held 1.2 million customers' personal information. In the same year, Bank of America, Wachovia, Commerce Bancorp, and PNC Financial Services Group detected illegal sales of account information by bank employees. Over 676,000 customers were affected by the internal breach in what was labeled at the time as potentially the "biggest security breach to hit the banking industry."[8]

### 2.2.1 Recent Florida Breaches

Companies operating within Florida are not immune to unintentional exposure or intentional breaches of customer information. The following list highlights several recent events in which customer information was exposed through unauthorized events.[9]

- In March 2005, Customer records of a Florida-based subsidiary of the LexisNexis Group were compromised when hackers used malicious programs to collect valid

[3] Figure 7a – 2006 national complaint data
[4] 2002 – 2005 national complaint data
[5] *2003 FTC Identity Theft Survey Report*
[6] 2003-2006 Figure 2, Complaint data-Florida
[7] *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress.* January 26, 2006. Retrieved July 11, 2007. www.ftc.gov/opa/2006/01/choicepoint.shtm
[8] *Bank Security breach may be biggest yet.* May 23, 2005. Retrieved July 2007. www.Money.cnn.com
[9] Compiled from Privacy Rights Clearinghouse Chronology of Data Breaches. Updated through Aug. 7, 2007. Retrieved August 9, 2007. www.privacyrights.org/ar/ChronDataBreaches.htm

customer ID passwords and to access the company's database. The hackers eventually gained access to 310,000 customer records.

- In February 2006, a contractor for Blue Cross and Blue Shield of Florida sent the names and social security numbers of current and former employees to his home computer, in violation of company policy. The former computer consultant was ordered to reimburse BCBS $580,000 for expenses related to the incident.

- In May 2006, hackers accessed the Vystar Credit Union in Jacksonville, FL. They collected the personal information of approximately 34,000 of its members, including names, social security numbers, dates of birth, and mother's maiden names.

- In April 2007, ChildNet, an organization that manages Broward County's child welfare system, had a laptop stolen by a former employee. The laptop contained social security numbers, financial and credit data, and driver's license information on approximately 12,000 adoptive and foster-parents.

- In June 2007, Jacksonville Federal Credit Union realized that social security numbers and account numbers of 7,766 of its members were accidentally posted, unencrypted, onto the Internet. The search engine Google indexed these records within its search criteria, exposing them throughout the World Wide Web.

- In July 2007, Fidelity National Information Services, of St. Petersburg, reported that 2,300,000 customer records were stolen by a worker from one of the company's subsidiaries. The information stolen included credit card and bank account numbers, and other personal information.

### 2.2.2 Potential of Exposure

The Privacy Rights Clearinghouse, a non-profit consumer information and advocacy organization, annually compiles a listing of all data breaches.[10] In review of the cases reported between 2005 to present, the majority of breaches can be categorized into four basic groups: technology, online exposure, insiders, and improper storage or disposal of customer records.

Technology exposure can include the unauthorized access into a company computer or server, especially those that store unencrypted, sensitive information. Also, this could include the unintentional downloading of malicious software to a company computer that is not secured with antivirus software.

Online exposure can include personal information that is inadvertently loaded onto the internet. Search engines, such as Google, can pick-up names through company Web sites and expose the information through the World Wide Web. Also, e-mails that include personal information may be sent to the incorrect addressee. Unencrypted e-mails may also be intercepted by hackers or malicious software.

[10] www.privacyrights.org/ar/ChronDataBreaches.htm

Insiders can be either dishonest employees whose intent is to commit fraud, or a well-intentioned employee who may commit an error in judgment. A dishonest employee can work for any corporation or agency. Employees with access to personal information may use extreme means to collect and steal personal information. Devices such as iPods, personal USB storage devices, and cell phones allow employees to collect and store data. This could include well-intentioned employees who take personal information off-site for work-related needs, but have the information stolen or lost while away from the office.

Improper storage or disposal can be an easy target for thieves looking for easy access to someone's personal information. This can include not only paper files that are left exposed, un-shredded, stolen, or improperly disposed, but also electronic files that are not maintained accordingly. Also, mailings that include exposed sensitive information could lead to a breach of information. Finally, disposal of discontinued office equipment could lead to a breach if electronic hard drives and memory devices are not properly "cleaned" prior to discarding the device.

## 2.3 Federal and State Authority

Several State and Federal statutes and initiatives govern data security and identify theft. These apply either directly or indirectly to Florida's electric utilities and should be considered in developing security practices and procedures.

### 2.3.1 Fair and Accurate Credit Transaction Act 2003

This amendment to the Fair Credit Reporting Act is designed to help elevate attention given to preventing identity theft. Two components of the law require companies to mask credit and debit card information on printed receipts, and to properly dispose of customer records. All credit card machines must be programmed to print only the last five-digits of the card information on a receipt, and may not include the expiration date.

The disposal requirements instruct businesses to properly dispose of documents containing customer information. Proper disposal includes burning or shredding of paper reports and erasing electronic storage devices. It can also include contracting the service out to a qualified disposal company.

### 2.3.2 Fair Debt Collections Privacy Act

This act limits the information that a creditor, or its agent, can provide to a third-party. It prevents a creditor, or its agent, from disclosing to a third-party that an individual is in debt. This law would prevent a utility from disclosing any past-due or charge-off information to any other than the customer of record or authorized user.

### 2.3.3 Florida Statute 817.568 and 817.5681

Florida Statute 817.568 makes it a state crime to fraudulently use another person's identifying information without first obtaining that person's consent.

### 2.3.4 Presidential Task Force of Identification Theft

In May 2006, President George W. Bush issued an Executive Order establishing the President's Task Force on Identity Theft. This task force, headed by the Attorney General and the Chairman of the Federal Trade Commission, was charged to "craft a strategic plan aiming to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution."[11] The task force's April 2007 strategic plan recognizes that "No single federal law regulates comprehensively the private sector or governmental use, display, or disclosure of social security numbers; instead, there are a variety of laws governing social security number use in certain sectors or in specific situations."[12] The task force has recommended the development of a comprehensive record on private sector use of social security numbers, including evaluating their necessity. The Task Force will make its recommendations by the first quarter of 2008. Until future recommendations are made, there are current federal and state laws in place that recognize and enforce the importance of safeguarding customer sensitive information.

## 2.4 Florida Public Service Commission Responsibility

Chapter 350.117 allows the Commission to conduct management and operation audits for any regulated company to ensure adequate operating controls exist. This report addresses whether each of the five companies audited for customer data security have proper controls in place. The audit particularly focused on management controls, information technology controls, user awareness, outsourcing controls, and auditing. Each of the following company chapters addresses these controls in a question and answer format.

[11] President's Task Force Strategic Plan p. viii
[12] President's Task Force Strategic Plan p. 24.

# 3.0 Florida Power & Light

Florida Power and Light Company (FP&L) is the largest investor-owned utility in Florida, providing service to over 4.4 million customers. The company has over 13,300 employees with approximately 600 FP&L customer service representatives. Company offices are located in Miami and Juno Beach.

## 3.1 Management Oversight

### Does Florida Power & Light management have a clear understanding that information security is a management responsibility?

Company responses to document requests and on-site interviews indicate that management has a clear understanding that information security is primarily a management responsibility, with many operational functions assigned to departments staffed with Subject Matter Experts. In this coordinated and cooperative effort, FP&L management seeks expert advice from senior information technology personnel, the legal department, corporate communications, corporate security officers, internal auditing, and IBM's Emergency Response Service. This open, ongoing exchange of ideas and assessed risk assists management in establishing the FP&L corporate climate and the priorities associated with company data security policies, practices, and procedures.

FP&L's goals and objectives for data security are: to provide a safe and secure working environment that allows maximum business flexibility and functionality, to meet all legal and regulatory requirements, and to protect customer sensitive information.

### What type of personal information does Florida Power & Light collect from customers?

FP&L employees use a customer service and billing system, the Customer Information System (CIS), to initiate new accounts, to update account information, and to store individual customer data. Most of these transactions occur by telephone. When initiating a new residential account, a customer service representative (CSR) collects information from the customer including the customer's full name, social security number, date of birth, address, phone number, and names of anyone authorized to discuss the account, such as a spouse or relative. Driver's license number, tax identification number, passport number, or an Alien Registration Number may be furnished in lieu of social security number. Should the customer decide to use the Automatic Bill Pay system, banking information would also be collected. Credit card numbers are not collected by FP&L.

## Has Florida Power & Light management assessed the appropriateness of the information collected from customers?

Responses to staff's data requests and interviews indicated that company management believes that the information currently collected from new customers is essential to processing customer requests and providing electrical services. Management is aware of the inherent danger in obtaining such information, especially individual social security numbers. FP&L management believes that, with appropriate management oversight and electronic network safeguards, risk of sensitive data compromise is reduced to acceptable levels. The social security number is specifically obtained in order to run a customer credit worthiness check. The number is then maintained for identification purposes and possible use if future non-payment results in a collection effort.

## Does Florida Power & Light adequately limit the use and disclosure of customers' personal information?

All FP&L employee access to the company database is password protected. Every employee must first use a log-on identification and password to get into the overall network. Then, those authorized to use the CIS system must again log-in and apply an additional password for further access. Automatic routines block a user following repeated incorrect entries. Failed entries are automatically captured, and a report of all failed log-in attempts is reviewed daily by network security personnel.

[redacted] FP&L management believes these measures, individually and collectively, combine to significantly increase network security and reduce the threat of compromise to sensitive customer information.

[redacted] After implementation, the company states that only those FP&L employees with a valid business need and the appropriate level of authorization will be allowed access to the full information.

[redacted]

[redacted]

## Do any employees have access to customers' personal information at off-site facilities?

FP&L has approximately 20 CSRs who work full-time from home. Management stated that these people are senior employees with exemplary work and conduct records, individuals who have met exceptional performance and professional standards to be afforded this privilege. Further, management reported assessing the work-from-home program, recognized what is perceived as an acceptably low risk of compromise to sensitive customer information, and believes sufficient controls have been placed in the program to compensate for such risk.

For instance, associates working from home must maintain a separate work environment to conduct FP&L business. The company considers separation critical to the prevention of distractions and minimizing the risk of compromising customer information. Any written material with sensitive customer information must be destroyed in accordance with the standards of *Records Management Procedure 810.1 – Transmitting, Declassifying, and Destroying Confidential Records*. The company contends that there is no need and no time for a CSR working from home to actually write anything when handling a call.

## What controls have Florida Power & Light put in place for remote access of customer personal information?

FP&L management states that it recognizes the inherent risk of employees having access to customer information outside the controlled security environment of the normal workplace. However, management believes this inherent risk, and increased difficulty of adequately safeguarding sensitive data outside the workplace, are acceptably mitigated by the exceptional quality of those chosen for the program. Home computer use is standardized and regulated by company policy. *Home Computer Use – Policy #13450* establishes guidelines and restrictions for use of company-provided computer equipment and software at home. The confidentiality of sensitive information must be protected from unauthorized use or viewing, including family members and home guests. Failure to comply can result in disciplinary actions, up to employee termination.

[redacted]

Along with its work-from-home associates, FP&L allows traditional associates the ability to access the company network from remote locations. Management states that because it is aware of the risks posed by remote access to sensitive data the access is very tightly controlled. Employees seeking access must request it and all remote access must be approved by the Information Technology manager. Once approved, access is made over a secure connection

allowing the user to open a virtual Windows desktop, run programs, and access servers. [redacted]

[redacted]

## 3.2 Information Technology Controls

### Has Florida Power & Light established an appropriate data security management function?

The Information Technology division (IT) has overall responsibility for all things pertaining to information security and management. The Director of IT Security heads the department. Immediately subordinate to the Director are three Technical Supervisors. IT assesses risk for the system and functionalities within the system, identifies and gauges potential vulnerabilities, and provides strategies to counter them. IT also monitors employee access to the network, network applications, programs, and electronically stored information. Employee system usage is monitored by IT, and the division processes changes to employee access based on changes in employment status.

### Has Florida Power & Light established appropriate information security policies, procedures, and guidelines?

FP&L IT management states that comprehensive security of sensitive customer information is impossible without a synergy between physical and virtual security. The IT division is responsible for all virtual information security measures and utilizes a layered 'defense in depth' to safeguard the network and the sensitive customer information it contains. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are in daily use. Encryption certificates currently in use for protection of all transmitted data are at the highest level, 128-bit.

As part of this layered protective defense, FP&L IT manages:

- Firewalls,
- Passive intrusion detection systems (IDS),
- Active intrusion prevention systems (IPS),
- Internet content filtering,
- Instant messaging protection,
- Scanning of perimeter devices,
- Virus protection, and
- BIGFIX, an application for vulnerability assessment and remediation.

Individual desktop workstations and servers are protected by:

- Standardized security configurations,
- Standardized security settings,
- Virus protection,

- A centrally managed upgrading effort, and
- The concept of "least privilege," limiting access to critical applications and sensitive information.

FP&L IT is also responsible for identifying all company applications and databases containing sensitive customer information. A list of these applications and databases is provided to all business units and regularly updated. IT conducts formal risk assessments of these applications and databases.

IT focuses additional efforts on application security by:

- Utilizing a formal software development life cycle (SDLC),
- Employing developer training for security coding,
- Conducting real time scanning of applications for vulnerabilities,
- Using a formal change management process for applications,
- Using a formal change management process for infrastructure,
- Producing security specific policies and procedures,
- Conducting about 20 security-specific internal audits annually, and
- Coordinating at least one external audit annually.

IT is responsible for compliance with applicable regulatory and legal obligations pertaining to security of sensitive information. FP&L has assigned a Senior Project Manager to direct and coordinate the efforts and products of the many departments involved in security compliance.

The FP&L Director IT Security, IM Project Manager, and IM Technical Supervisors believe the company has a full and comprehensive set of policies relating specifically to data security. The list includes:

- *#13330 - Security Update, Patch Management Policy and Requirements,*
- *#13240 - Incident Response for Cyber Attack,*
- *#13255 - Malware Protection and Requirements,*
- *#13260 - Network Security,*
- *#13260.2 - Network Security – Wireless Networks,*
- *#13260.4 - Network Security – Access & Connectivity,* and
- *#13265 -Remote Control Capability.*

FP&L's change management process for network software updates is controlled by Policy #13330 *Security Update, Patch Management Policy and Requirements.* This policy defines policy objectives, patch management exceptions, the applicable systems, roles and responsibilities, the risk assessment process, incident response protocols, key definitions, and related references.

The IT Manager sits on the Change Review Board. On this board, and in the change management process, the IT Manager serves as the subject matter expert for the network structure, operation, data security, and all applications in use on the network.

The IT staff seeks to protect information, including customer sensitive data, by making the network as impervious to hostile penetration as possible. This effort is led by installing the most current versions of vendor upgrades. Such upgrades are commonly called "patches."

[redacted]

Company personnel charged with securing sensitive customer information utilize a combination of virtual and physical measures for data protection. Many routine operations containing customer data feature automated safeguards, such as the masking of information.

Managers and supervisors routinely monitor employee access to sensitive information. Reporting changes in an employee's status or business need to access sensitive customer data is required by policy so that immediate revision of access rights can be accomplished.

**Does Florida Power & Light limit physical access to customer information data resources through access authorization procedures, monitoring devices, and alarm systems?**

FP&L has two Florida-based customer service sites in which CSRs provide service and collect information from account holders, and a facility in El Paso, Texas operated by a third-party vendor. The Florida sites are located in Miami and West Palm Beach. Approximately 600 CSRs work from these two sites, with roughly 60 percent in the Miami office. The El Paso site is staffed by approximately 100 vendor personnel. Personnel access to every customer call center is controlled. There is either a security gate, a door which opens only with a magnetically coded key card, or security personnel at the front door. Visitors are few, must have management authorization to enter the site, and are escorted from arrival to departure at each facility.

In a virtual sense, these three sites function as a single center, seamless to the customer calling in to make an inquiry. The Miami center operates 24 hours per day, seven days per week. Centers located in West Palm Beach and El Paso operate on a reduced schedule. West Palm Beach and El Paso receive only general questions, but do have access to sensitive customer information.

FP&L handles its own payment processing operations. The bulk of these operations are performed [redacted] The site is secure, access is controlled; visitors are rare and must be escorted. The payment processing unit is located several floors above the main level of the FP&L building, isolated, and with minimal access points.

The FP&L IT facility [redacted] and access is tightly controlled. Any employee seeking access must have a need verified by IT. Each person with an established need is then issued a magnetically coded card. The card allows access to the bearer when it is slid through a corresponding magnetic lock located on the access door. Use of a magnetic system allows access to be controlled and monitored, both in real time and for

subsequent auditing purposes. Besides IT personnel, only the company president is authorized unescorted access.

### Does Florida Power & Light restrict access to customer information related software functions, data, and programs?

FP&L managers state that the company uses the principle of "least privilege" and "need to know" in allocating access rights. Employees are designated for access only to those areas of the network in which they have a legitimate business need to adequately perform their job requirements. Management contends that other access is denied.

System changes will be implemented to increase masking of customer information, and access will be restricted to only those users specifically defined as requiring non-public information to conduct business. [redacted]

### Does Florida Power & Light monitor software security activity and produce appropriate management reports?

FP&L IT analysts monitor network access in real time. This monitoring activity captures information on which employees are logged on to the network, what network areas are accessed, when the access occurred, duration of the access, and whether unauthorized users attempted access.

The information management system has controls that automatically monitor, capture, and record employee software activity and network access for later use in risk assessment and audits. IT personnel, department supervisors, and company management regularly review the results. Such information is also available on short notice via a request to IT.

## 3.3 User Awareness and Training

### Does Florida Power & Light have adequate privacy and data security policies and procedures?

FP&L employs a combination of written policies, practice, and procedures to provide a structured framework for customer data security. All company policy and procedure statements are current. FP&L policies, practices, and procedures demonstrate senior management's concern for the security of customer sensitive information while delineating and subordinating functional security responsibilities within the company. Handling of sensitive customer information is emphasized and standardized throughout the company.

According to FP&L management, privacy and data security policies, employee practices, and company procedures are comprehensive in nature, regularly reviewed and updated as required. Certain key policies are annually revisited and acknowledged by all employees.

Answers to staff's document requests demonstrate that protecting sensitive customer information is integral to FP&L's goals and objectives. Employees observed by staff seemed genuinely concerned with safeguarding the sensitive information entrusted to them.

Every employee must annually sign a statement acknowledging that they have read and understand the company *Code of Ethics*. This code details employee responsibility for protection of proprietary and confidential information. Included in the scope of this code is the principle of protecting non-public customer information. Disclosure of such information to anyone outside FP&L, without specific authorization by the company, is strictly prohibited. In addition to the *Code of Ethics*, each employee must also read and sign a separate confidentiality agreement as part of the hiring process, and undergo a background check and drug screening.

FP&L management believes the company has a full and comprehensive set of policies relating specifically to data security. Along with the policies previously shown in Section 3.2, the following are also applicable to data security:

- *#13010* - *Information Protection Policy,*
- *#13020* - *Information Security Violations,*
- *#13050* - *Access to Critical/Sensitive Systems,*
- *#13270* - *Remote (Dial-Up) Access,* and
- *#13450* - *Home Computer Use.*

## Are Florida Power & Light employees properly trained on privacy and data security policies?

FP&L's goal for employee training is that all new employees understand the underlying need for data security, the regulatory and legal requirements to safeguard sensitive information, and to be aware of continually evolving threats posed to confidential information by electronic spam, viruses, and phishing. The company seeks to accomplish this goal through intensive security instruction for new hires, annual refresher training, area specific training (especially for regulatory and legal requirements), periodic awareness bulletins, and universal e-mail updates and warnings.

New hire instruction is conducted in a variety of formats, such as small group sessions, one-on-one, and company intranet. Annual refresher training is usually conducted either by instructors, in person or via teleconference, or self-paced intranet lessons. New customer service representatives are required to take a tutorial online called "*Safeguarding Customer Information.*" This tutorial is self-paced and includes a skills assessment. The tutorial usually takes an employee 20 to 25 minutes to complete.

Each employee receives training on the *Policy #13010--Information Protection.* This provides an explanation of the minimum requirements, individual responsibilities, and actions expected of employees to safeguard FP&L's information resources and services. The policy is applicable to all employees. *Policy #13010--Information Protection* emphasizes the minimum requirements, responsibilities, and metrics for protection of information. The procedures contained in the policy are applicable to every FP&L network user, and are also relevant to

information and files on the network, subsystems, servers, workstations, telephones, mainframes, host computers, and local or wide area networks.

Approximately 25 additional policies, practices, and procedures relevant to data and system security are included in new employee training. Included in this additional training is a wide variety of policies and subjects such as *Policy #13020--Information Security Violations, Policy #13030--System Access Confidentiality, Policy #13050--Access to Critical/Sensitive Systems, Policy #13260--Network Security,* and *Policy #13260.2--Network Security – Wireless Networks.*

### Does Florida Power & Light have policies and procedures in place which address penalties for violations of Privacy or Data Security policies?

FP&L *Policy #13010 - Information Protection* clearly outlines company data security protocols and the applicability to all employees. All individuals, groups, and organizations identified in the scope of the policy are responsible for full understanding and compliance. It holds management (at all levels) accountable for ensuring compliance that the policy is effectively communicated to subordinates and universally understood. Failure to comply without first obtaining an approved exception from IT will result in a sliding scale of corrective or disciplinary action based on severity of the offense. Employees can find a full explanation of possible corrective or disciplinary action(s) in *Policy #13020 - Information Security Violations.*

According to FP&L management, any breach in properly securing sensitive customer information will result in immediate coaching and possible retraining under the *"Performance Toward Excellence"* program. The program is based on the severity of the infraction; the more serious the violation, the more formal the retraining and reassessment program. Corrective or disciplinary actions generally increase from oral to written counseling, reassessment and the employee affirming his or her commitment to the company, probation, and then termination.

## 3.4 Outsourcing Controls

### Does Florida Power & Light provide third parties with access to customer personal and/or banking information?

Florida Power & Light contracts with an independent vendor operating in El Paso, Texas to provide customer services. In a virtual sense, this site functions as a single customer service center with the two Florida locations, seamless to a customer calling in to make an inquiry. The center in El Paso operates on a reduced schedule and processes only general customer service questions. There are approximately 100 customer service representatives working from this facility who currently have access to customer information. FP&L managers stated that the number of personnel with access in El Paso will be significantly reduced in 2008.

For bill payment, FP&L also currently has a network of 363 authorized pay agent locations using the Online Pay Agent Locations (OPAL). OPAL is an automated payment processing system which communicates payment information in real time to the FP&L

mainframe and CIS from the remote location. OPAL cannot query CIS for social security numbers or driver's license numbers. However, it does have the ability to obtain limited customer information specifically required to process payments. OPAL also automatically updates the customer's payment record. Each off-site payment agent signs an agreement with FP&L that includes nondisclosure and confidentiality terms.

Agents scan the billing coupon on OPAL, capturing the customer account information, which is verified by CIS. Once verified, OPAL identifies account status (active, final, disconnected, etc.) and makes this information available to the agent. Should the customer not have a coupon, or the agent not have a scanner, the agent will manually key in the account number to OPAL in order to perform the account verification.

### What controls has Florida Power & Light put in place to prevent disclosure of customers' personal information by third parties?

FP&L does allow third-party contractor access to internal systems. The company takes the following steps to safeguard sensitive customer data and prevent unauthorized access:

- Requires a confidentiality agreement to be signed by the third-party,
- Uses a formal process to determine appropriate system level access,
- Provides only the access determined appropriate by the process,
- Validates system access requests,
- Regularly audits third party procedures,
- Logs system access for review and possible investigation,
- On-site surveys to evaluate vendor's ability to protect customer data,
- Provides customer service training for system interaction, and
- Complies with best practices for processing and accessing customer information (*Center for Internet Security Standards*).

The vendor CSR agents working in the El Paso call center are required to undergo the same training and testing as FP&L employees and must sign an identical confidentiality agreement. Those customer service representatives working from the El Paso center are only assigned generalist questions and have no access to sensitive customer information. FP&L management provides the same sort of supervisory oversight of customer service operations in the El Paso center as in Miami and West Palm Beach, electronically and through periodic site visits/audits. El Paso vendor personnel must undergo a background check identical to that for FP&L employees.

## 3.5 Auditing Controls

### Does Florida Power & Light possess, or have access to, competent auditing resources to evaluate information security and associated risks?

FP&L auditing is the responsibility of the Vice-President for Internal Auditing. Immediately subordinate to the VP are four Auditing Managers. There are 32 full-time internal

auditors on the staff. Of these, eight positions have specific information security backgrounds and are assigned to perform IT audits.

Staff reviewed confidential management reports, as well as internal and external audit reports for the last 24 months. Several security risks of varying severity were reported. Of the whole, few rose to the level of medium risk and fewer still to high risk. Medium and high risks were prioritized for remediation, plans developed, and timelines established. The company states that funds were allocated, personnel were assigned to the remediation effort, and management actively monitored progress until completion.

## Does Florida Power & Light periodically assess the organization's information security practices?

On average, IT management schedules and conducts approximately 22 internal audits annually. These audits focus on the overall security of the system or the data stored on it. Audits generally include components designed to review information security even if the audit is not specifically focused on data protection. Audit results are used to assist FP&L in assessing the viability of its data security systems. IT also stages unscheduled penetration tests throughout the year to validate its intrusion detection systems, intrusion protection systems, and electronic firewalls.

The company has performed over 40 internal and external audits on its general network and sensitive data security procedures in the period covered by this report. This is more than any other investor-owned electric provider associated with this review. Frequent audits of information security processes assist FP&L in assessing the overall state of its data security systems. Auditor reports help the company devise the most relevant information, security policies and procedures, prioritize needs, and budget appropriately. FP&L management were proactive in conceiving, funding, scheduling, and implementing appropriate remedial actions for information security risks discovered during internal and external audits.

## Has management provided assurance that information security breaches and conditions that might represent a threat to the organization will be promptly made known to appropriate Florida Power & Light corporate and IT management?

FP&L has such a notification process currently in place. Policy #13240 *Incident Response for Cyber Attacks* specifically addresses those actions which must be taken in the event of attacks on the network or on sensitive information. Company management reaffirmed that one of the steps required by this policy is to provide notice immediately to the IT internal audit department of any actual, attempted, or suspected unauthorized network access. Conditions and circumstances which represent a potential threat of compromise must also be reported, such as theft of equipment.

The company reported that it has not experienced, or is aware of, any breaches to sensitive customer information during the past 24 months, the period of this review.

## 3.6 Conclusions

Florida Power & Light has developed policies, practices, and procedures focused on protecting sensitive customer information. Company management acknowledges its responsibility for information security. Staff believes that the positives associated with efforts to safeguard sensitive customer data outweigh the negatives. Virtual and physical security controls currently in place are in keeping with industry practices, layered for a defense in depth, and effective overall. FP&L is in compliance with applicable state, federal, and industry requirements regarding the protection of sensitive customer information.

[redacted]

[redacted] Access will also be further restricted to users having a validated business need to regularly access such data. Staff believes reducing this level of access will substantially decrease risk of compromise.

[redacted] After implementation, only those FP&L employees with a valid business need and appropriate level of authorization will be able to see the full information. [redacted]

[redacted]

CONFIDENTIAL

# APPENDIX A

## GLOBAL TECHNOLOGY AUDIT GUIDE (GTAG)

GTAG's privacy best practices are derived from a variety of worldwide sources and were central to staff's review. These privacy best practices support prudent data security management and reduce risk for those companies that routinely use these techniques as part of their overall corporate plan. The privacy best practices considered during this review include:[13]

- Performing adequate and regular privacy risk assessment;
- Establishing a privacy officer or organization to serve as the focal point for coordination of privacy activities and the handling of complaints or issues;
- Developing awareness around key data handling and identity theft risks;
- Masking personal identification numbers, such as social security numbers, and other sensitive information when possible;
- Supervising and training call center staff to prevent social engineering and similar risks;
- Managing marketing lists and all third-party vendor relationships effectively;
- Creating awareness of Web and e-mail vulnerabilities;
- Developing record retention and destruction policies;
- Implementing a data classification scheme based on the sensitivity and data mapping;
- Conducting risk assessments of access controls, physical security access restrictions, and change controls;
- Implementing intrusion detection and prevention technologies;
- Completing penetration testing and independent testing/review of key controls, systems, and procedures; and
- Limiting data collection to operationally necessary data.

[13] Global Technology Audit Guide, "Managing and Auditing Privacy Risks." The Institute of Internal Auditors. p. 15-16, June 2006

# APPENDIX B

## CUSTOMER DATA SECURITY INFORMATION

Florida investor-owned utilities have programs designed to safeguard sensitive customer information. These programs are multifaceted, combining written policies, employee procedures, and management or supervisory practices. A variety of virtual and physical safeguards round out the data security system found in each company.

This chart summarizes each company's security policies, practices, and initiatives. These points are discussed in more detail in each respective company chapter.

**Florida Investor-Owned Utilities' Customer Data Security Information**

| | FPL | FPUC | GPC | PEF | TEC |
|---|---|---|---|---|---|
| Emphasis on data security (new employee training, ethics standards, instruction/ statements, coaching, and supervision) | | | | | |
| Proactive data security programs (IT, Customer Service, Payment Processing) | | | | | |
| Audit of IT / Customer data in the last 24 months | | | | | |
| Number of security breaches, last 24 months | | | | | |
| Number of IT auditors | | | | | |
| Employs IT "defense in depth" using a combination of Intrusion Detection, Intrusion Prevention, virtual and physical measures to counter risks | | | | | |
| Masking of customer social security numbers (SSN) | | | | | |
| Total number of employees | | | | | |
| Number of employees with access to customers' full social security number | | | | | |
| Percentage of employees with access to customers' full social security number | | | | | |
| Number of employees with access to customers' banking account information | | | | | |
| Percentage of employees with access to customers' banking account information | | | | | |
| Number of employees with access to customers' date of birth information | | | | | |
| Work-at-home program for Customer Service Representatives | | | | | |
| Share customer information with an authorized third party over the telephone | | | | | |

*Source: Company Responses to Staff Document Requests 1 and 2*

# APPENDIX C

## TREATMENT OF SENSITIVE CUSTOMER DATA

Florida investor-owned utilities collect, use, and mask a variety of sensitive customer information. Collection, use, and masking of information in each company is controlled and safeguarded by a combination of written policies, employee procedures, and management supervision practices. Virtual and physical security measures in each company round out the system designed to protect the data. The following chart summarizes the information each company collects, uses, and masks.

| | Collects | Uses | Masks |
|---|---|---|---|
| **FP&L** | | | |
| Social Security Number | | | |
| Driver's License Number | | | |
| Bank Account | | | |
| Date of Birth | | | |
| Credit Card Info | | | |
| **FPU** | | | |
| Social Security Number | | | |
| Driver's License Number | | | |
| Bank Account | | | |
| Date of Birth | | | |
| Credit Card Info | | | |
| **GULF** | | | |
| Social Security Number | | | |
| Driver's License Number | | | |
| Bank Account | | | |
| Date of Birth | | | |
| Credit Card Info | | | |
| **PEF** | | | |
| Social Security Number | | | |
| Driver's License Number | | | |
| Bank Account | | | |
| Date of Birth | | | |
| Credit Card Info | | | |
| **TEC** | | | |
| Social Security Number | | | |
| Driver's License Number | | | |
| Bank Account | | | |
| Date of Birth | | | |
| Credit Card Info | | | |