080061-EI

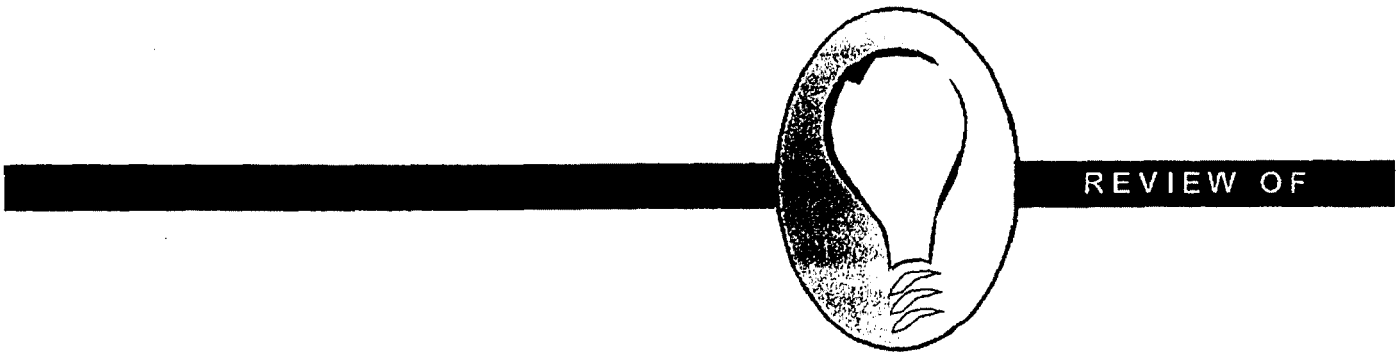
Exhibit B

REDACTED

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

DOCUMENT NUMBER-DATE
10909 DEC 13 08
FPSC-COMMISSION CLERK

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

1.4.4 Progress Energy Florida (PEF)

PEF appropriately places an emphasis on protecting confidential customer information. The company's procedures and employee training programs provide detailed and specific guidelines on safeguarding information. The company secures its facilities and work units to deter unauthorized access. Along with strong policies and procedures regarding confidentiality, the company's Information Management division has emphasized reducing the company's exposure to internal and external security threats.

Staff has concerns about some aspects of PEF's practices and procedures employed to safeguard sensitive information. The most concerning issues are:

- [redacted] 1
- [redacted] 2

1.4.5 Tampa Electric Company (TEC)

CONFIDENTIAL

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]

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]

[redacted] PEF management states that three associates have been trained to use this software; [redacted]

Additionally, PEF maintains locked disposal bins at its call centers for associates to dispose of any printed or written confidential information. These bins are collected and the material is shredded by a disposal vendor.

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

PEF allows supervisors to remotely access the Progress Energy network. This authorization must be approved by the Information Management unit. Once an associate successfully logs into the network via a remote location, they are able to access the normal software applications that are available while on-site. This includes the ability to access any normally authorized account software, including customer personal information. PEF does not have a work-from-home program that allows associates to perform normal job duties off-site.

What controls has Progress Energy Florida put in place for remote access of customer personal information?

[redacted]

6.2 Information Technology Controls

Has Progress Energy Florida established an appropriate data security management function?

PEF management places the responsibility of protecting customer information within its Information Technology Division. Within the Information Technology Division, the company has under the director a Manager of Security Services. This position is responsible for ensuring that the overall network system is secure and protected from unauthorized access. The Manager of Security Services has 15 analysts who work to ensure the system is secure.

Has Progress Energy Florida established appropriate information security policies, procedures, and guidelines?

Progress Energy employs a defense in depth approach to its system architecture. It has designed a system with a strong perimeter, internal monitoring, and a philosophy of least privilege in which only associates whose job requires certain information have access to that information. [redacted] 1 2 3 4

The company has a series of policies and procedures that addresses the overall security of the network, along with individual application and components. Specific procedures include, but are not limited to:

- Overview-IT Security Standards,
- Access Control,
- Application Security,
- Cyber Security,
- Database Security,
- Network Security,
- Resource Monitoring,
- Security Awareness and Training,
- Virus Protection, and
- Workstation Security.

These policies provide the company standards for securing and monitoring the security of the network. Each is available to the IT associates via the company's online training and procedure manual.

[redacted] 5 6 7 8 9 10 11

Does Progress Energy Florida limit physical access to customer information data resources through access authorization procedures, monitoring devices, and alarm systems?

PEF provides a secure environment for its employees and network facilities. Each of the company facilities is monitored with security guards and requires key card access into restricted areas. Each associate's key card is programmed to grant access on an as-needed basis. The

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. 1

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. [redacted] 2 3 4 5

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.

6.4 Outsourcing Controls

Does Progress Energy Florida provide third parties with access to customer personal or banking information?

PEF outsources a portion of its customer inquiries to a vendor call center [redacted] This call center assists PEF by handling general account inquiries and payment arrangements. Using an initial screening menu, PEF segregates incoming calls based on service type. The contract associates do not establish service, but have access to the CSS account and billing records. These contract associates do have the ability to make payment arrangements and accept credit card payments over the phone. 1

PEF also allows its remittance processing software vendor access to its payment processing system to make any necessary modifications or adjustments. This system is a stand-alone server that only houses the payment receipts and account numbers. The vendor does not have access to the billing and payment system that houses customer identifying information.

PEF also has contract agreements with two vendor pay agents. These vendors have multiple payment locations within PEF's territory. These vendors can collect payments, but do not have access to the CSS system or specific customer information.

PEF accepts credit card payments and has a contract with [redacted] for its credit card payment processing. Customers can make a credit card payment using [redacted] automated phone response unit, via its Web site, or by directly calling a service representative. The CSS system does not maintain the credit card information once the transaction is processed through [redacted]. 2 3 4

What controls has Progress Energy Florida put in place to prevent disclosure of customers' personal information by third parties?

PEF states that it's contracted and vendor associates must submit to the same background and drug screen requirements as PEF associates. The company states that contracts with vendors always include a confidentiality clause to protect customer information and a right-to-audit clause. The vendor associates [redacted] are monitored and evaluated by PEF management on a continuing basis to verify compliance with company standards and expectations. [redacted] 5 6 7

6.5 Auditing Controls

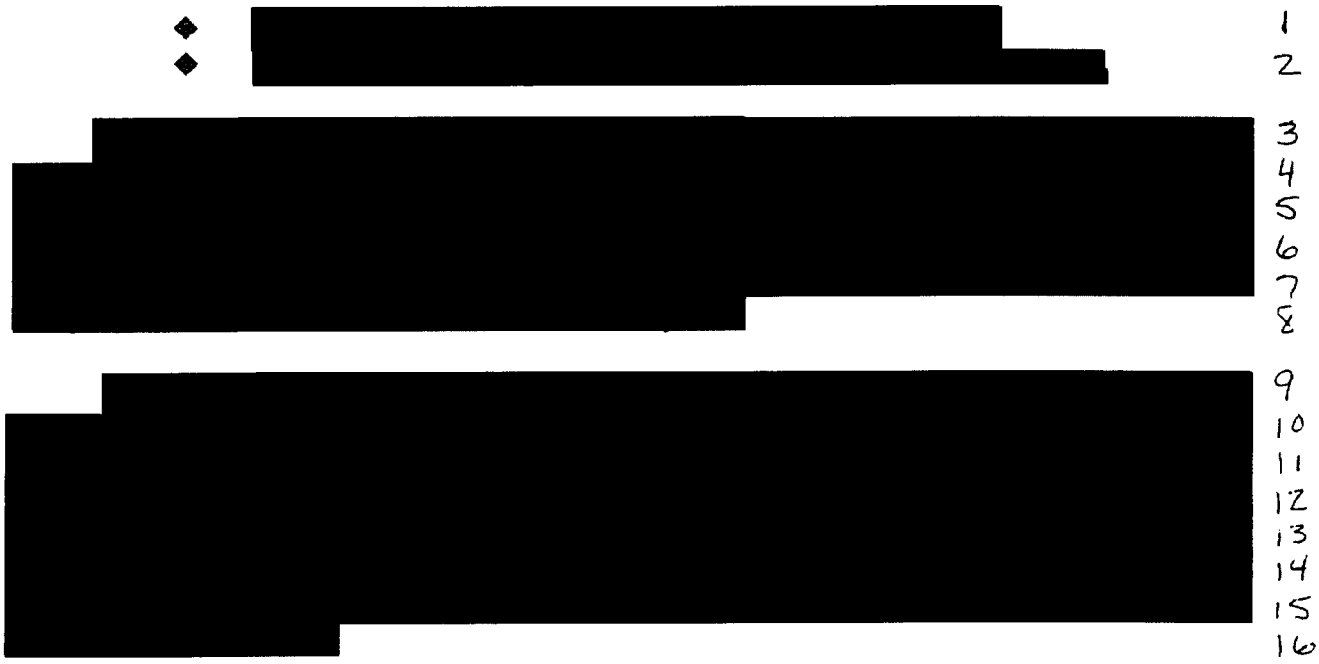
Does Progress Energy Florida possess, or have access to, competent auditing resources that evaluate information security and associated risks?

The audit groups use both risk-based and cycle-based approaches to developing the company's audit plan. Progress Energy has an internal audit unit that focuses on four areas:

6.6 Conclusions

PEF appropriately places an emphasis on protecting confidential customer information. The company's procedures and employee training programs provide detailed and specific guidelines on safeguarding information. The company secures its facilities and work units to deter unauthorized access. The company monitors and restricts admittance to its buildings and, as with the remittance processing unit, restricts access to specialized areas by job type. Along with strong policies and procedures regarding confidentiality, the company's Information Management division has emphasized reducing the company's exposure to internal and external security threats.

Staff has concerns about some aspects of PEF's practices and procedures employed to safeguard sensitive information. The most concerning issues are:



CONFIDENTIAL

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).				[redacted]	
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

CONFIDENTIAL

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			

Attachment B (DR-1)

REDACTED

(25 pages)

PEF's Responses to IOU Data Security Review Request (DR-1)
Undocketed

Attachment C (DR-1)

REDACTED

(2 pages)

Attachment D (DR-1)

REDACTED

(1 page)

Attachment F (DR-1)

REDACTED

(6 pages)

PEF's Responses to IOU Data Security Review Request (DR-1)
Undocketed

Attachment G (DR-1)

REDACTED

(3 pages)

Attachment H (DR-1)

REDACTED

(1 page)

Attachment J (DR-1)

REDACTED

(3 pages)

Response to Data Request 2

REDACTED

(14 pages)

PEF's Responses to IOU Data Security Review (DR-2)
Undocketed

Bureau of Regulatory Review Workplan
Progress - IOU Data Security Review

Ref No.	Task	Audit Hours	Standard	Audit Notes	Finding
	overall system data integrity. Evaluate the company's approach to reducing these risks and the overall impact on performance		should evaluate the risks and develop a model to reduce and overcome these risks. The company should evaluate how these risks impact and inhibit overall performance.	industry to evaluate the risk to the company and customer. The company provided a copy of its risk assessment for customer data—"Privacy Audit Initiatives"	
D	Document the internal controls established by the company to protect its overall system integrity. Evaluate the adequacy of these controls		Management should develop internal controls based on the risks associated with its system integrity. These controls should allow the company to reduce its exposure to potential loss of information.	[redacted]	
E	Assess the adequacy of the management control system for measuring, reporting, and monitoring data		Management should continually monitor the company's compliance with its data security initiatives. The company should document	The company does have a series of controls to monitor and verify who have access to customer information. The company routinely verifies its user ID access.	

Bureau of Performance Analysis
PEF - Document Summary and Control Log

Company:	PEF	Workload Control #:	PA-07-05-005
Area:	Data Security	File Name:	Document Summary two- PEF.doc
Auditor(s):	Coston, Rich		

Document #: 2.1 Date Requested: Date Received: Comments: (i.e., Confidential) **ALL** **CLAIMED** **CONFIDENTIAL**	**Document Title and Purpose of Review:** 1. Please explain how the company complies with requirements of: a. FACTA (Fair and Accurate Transactions Act) b. Right to Financial Privacy Act c. Drivers License Protection Act d. Consumer Information and Records Disposal Act e. Health Insurance Portability and Accountability Act of 1996 f. Florida Statute 817.5681 2. Please describe how PEF ensures compliance by its third party customer service vendors and its affiliated company with the above mentioned acts?
	Summary of Contents: A: [redacted] B: C: D: F:
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required:
Document #: 2.2 Date Requested: Date Received: Comments: (i.e., Confidential)	**Document Title and Purpose of Review:** 2. Please describe how PEF ensures compliance by its third party customer service vendors and its affiliated company with the above mentioned acts?

	Summary of Contents: [redacted] **Conclusions:** **Data Request(s) Generated:** No. _____ Description: No. _____ Description: **Follow-up Required:**
Document #: 2.3 **Date Requested:** **Date Received:** **Comments: (i.e., Confidential)** **ALL** **CLAIMED** **CONFIDENTIAL**	The response to DR-1, Q-13 cited no *customer-initiated* complaints or allegations regarding security of sensitive data. Please provide incident details and remedial action specifics of **company-discovered** security breaches from January 2005 through the present for: a. Customer credit card information b. Customer bank account information c. Customer Social Security Account Number d. Customer drivers License Number e. Theft / loss of company laptop computers f. Theft / loss of company portable storage (CD, disk, hard drive, etc) **Summary of Contents:** [redacted] **Conclusions:** **Data Request(s) Generated:** No. _____ Description: No. _____ Description: **Follow-up Required:**
Document #: 2.4 **Date Requested:** **Date Received:** **Comments: (i.e., Confidential)**	**Document Title and Purpose of Review:** Is there currently a policy regarding introduction of personal electronic equipment into the workplace (e.g. cameras, voice recorders, camera-equipped cell phones or PDA devices, flash / jump drives, etc). If so, please provide a copy of the policy. **Summary of Contents:** [redacted]

[redacted]

Conclusions:

Data Request(s) Generated:
No. _____ Description:
No. _____ Description:

Follow-up Required:

Document #: 2.5
Date Requested:
Date Received:
Comments: (i.e., Confidential)

ALL

CLAIMED

CONFIDENTIAL

Document Title and Purpose of Review:
Please complete the chart below, indicating the applicable current programs or procedures with an "X" in the appropriate box. Provide explanatory comments as needed.

Collect customer SSAN	Mask or encrypt SSAN	Collect customer Drivers Lic #	Mask or encrypt DL #	Collect bank acct info	Mask or encrypt bank info	Collect credit card info	Mask or encrypt credit card info	Collect date of birth	Mask or encrypt date of birth

Summary of Contents:
[redacted]

Conclusions:

Data Request(s) Generated:
No. _____ Description:
No. _____ Description:

Follow-up Required:

Document #: 2.6
Date Requested:
Date Received:
Comments: (i.e., Confidential)

Document Title and Purpose of Review:
Please provide the number of associates in the company, holding company, and affiliated company who have access to customer:

a. full Social Security Number
b. maintained Banking/credit card information
c. date of birth

Summary of Contents:
[redacted]

	[redacted]
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required:
Document #: 2.7 Date Requested: Date Received: Comments: (i.e., Confidential) **ALL** **CLAIMED** **CONFIDENTIAL**	**Document Title and Purpose of Review:** Please provide the number of contracted third-party associates who have access to customer: a. full Social Security Number b. maintained Banking/credit card information c. date of birth
	Summary of Contents: [redacted]
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required:
Document #: 2.8 Date Requested: Date Received: Comments: (i.e., Confidential)	**Document Title and Purpose of Review:** Please describe how the company monitors the deposal of customer information for affiliated associates who assist with PEF customer inquires
	Summary of Contents: [redacted]
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required:
Document #: 2.9 Date Requested: Date Received:	**Document Title and Purpose of Review:** In DR 1 response attachment J, please describe the chart and explain the reasoning and impacts of the "Business Continuity" percentage reporting as off-target.

Comments: (i.e., Confidential) **ALL** **CLAIMED** **CONFIDENTIAL**	 **Summary of Contents:** [redacted] **Conclusions:** **Data Request(s) Generated:** No. _____ Description: No. _____ Description: **Follow-up Required:**
Document #: 2.10 **Date Requested:** **Date Received:** **Comments: (i.e., Confidential)**	**Document Title and Purpose of Review:** Has all of the action plans for the December 2006 audit been completed? If not, please provide a status and new target completion date. **Summary of Contents:** [redacted] **Conclusions:** **Data Request(s) Generated:** No. _____ Description: No. _____ Description: **Follow-up Required:**

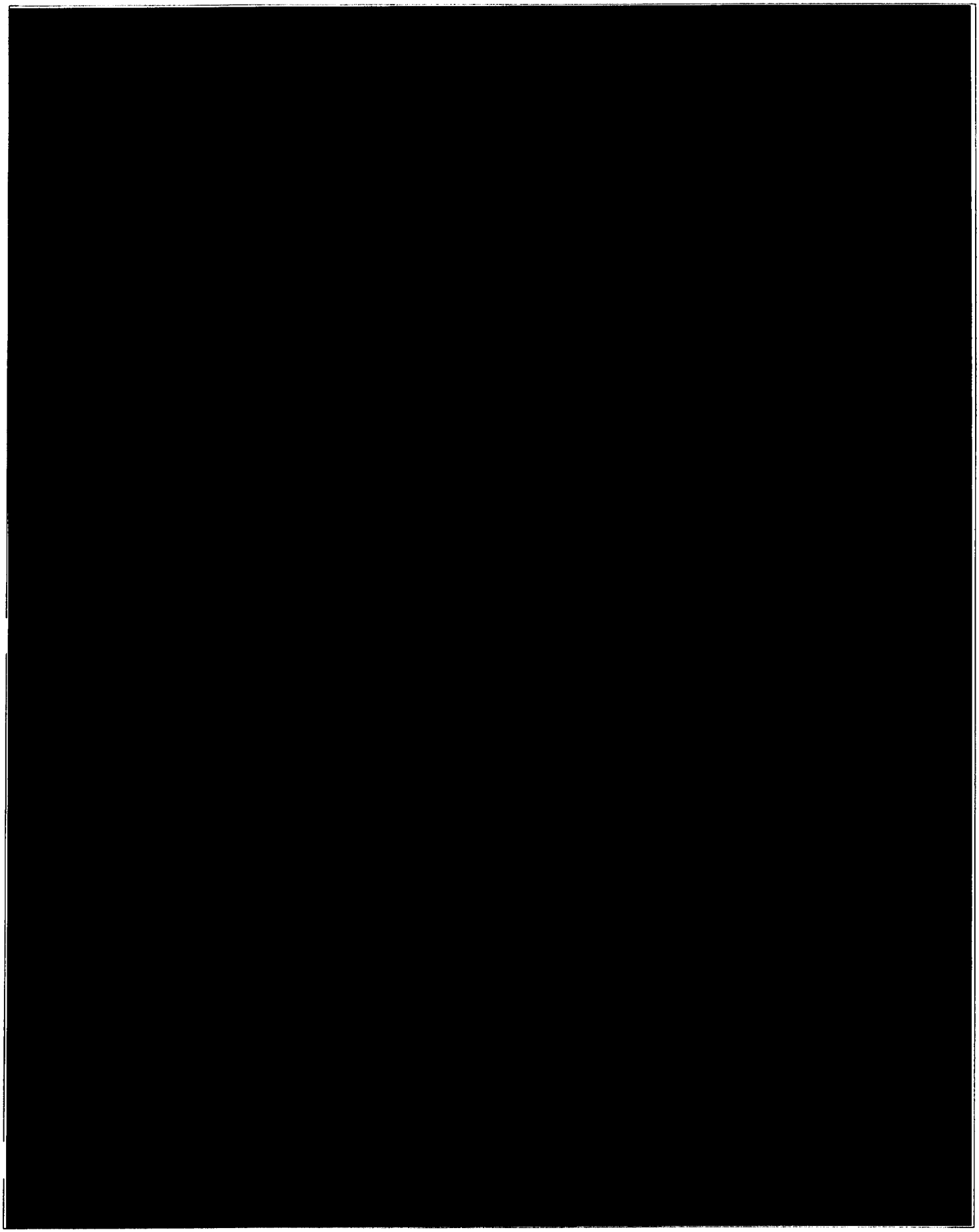
Bureau of Performance Analysis
Interview Summary

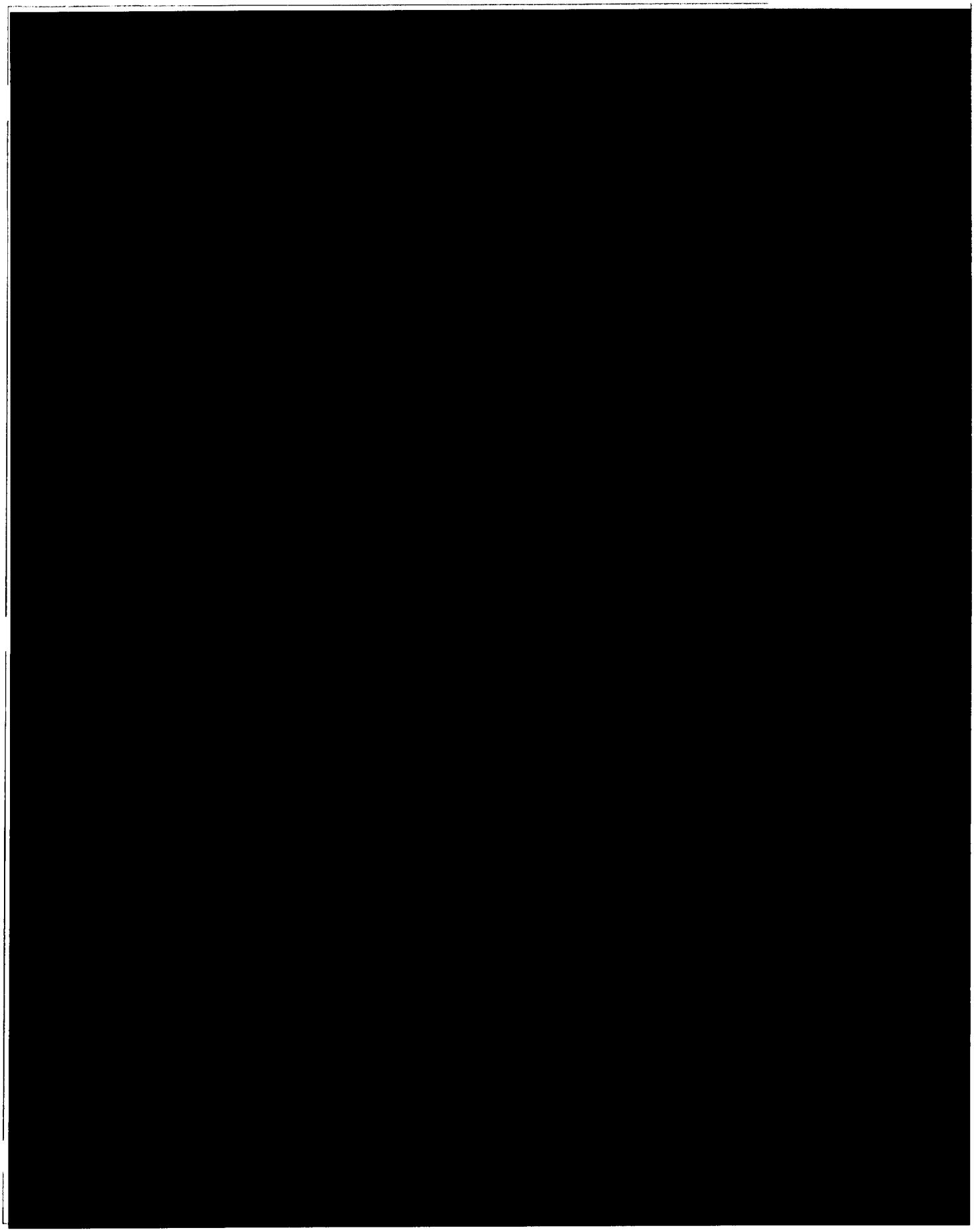
Company: Progress Energy-Florida	Interview Number: File Name:
Name: Elaine McCallister, sr. Financial Analyst, Customer Services Operations	Date of Interview: August 8, 2007 PEF Clearwater-Bayview offices Clearwater, FL

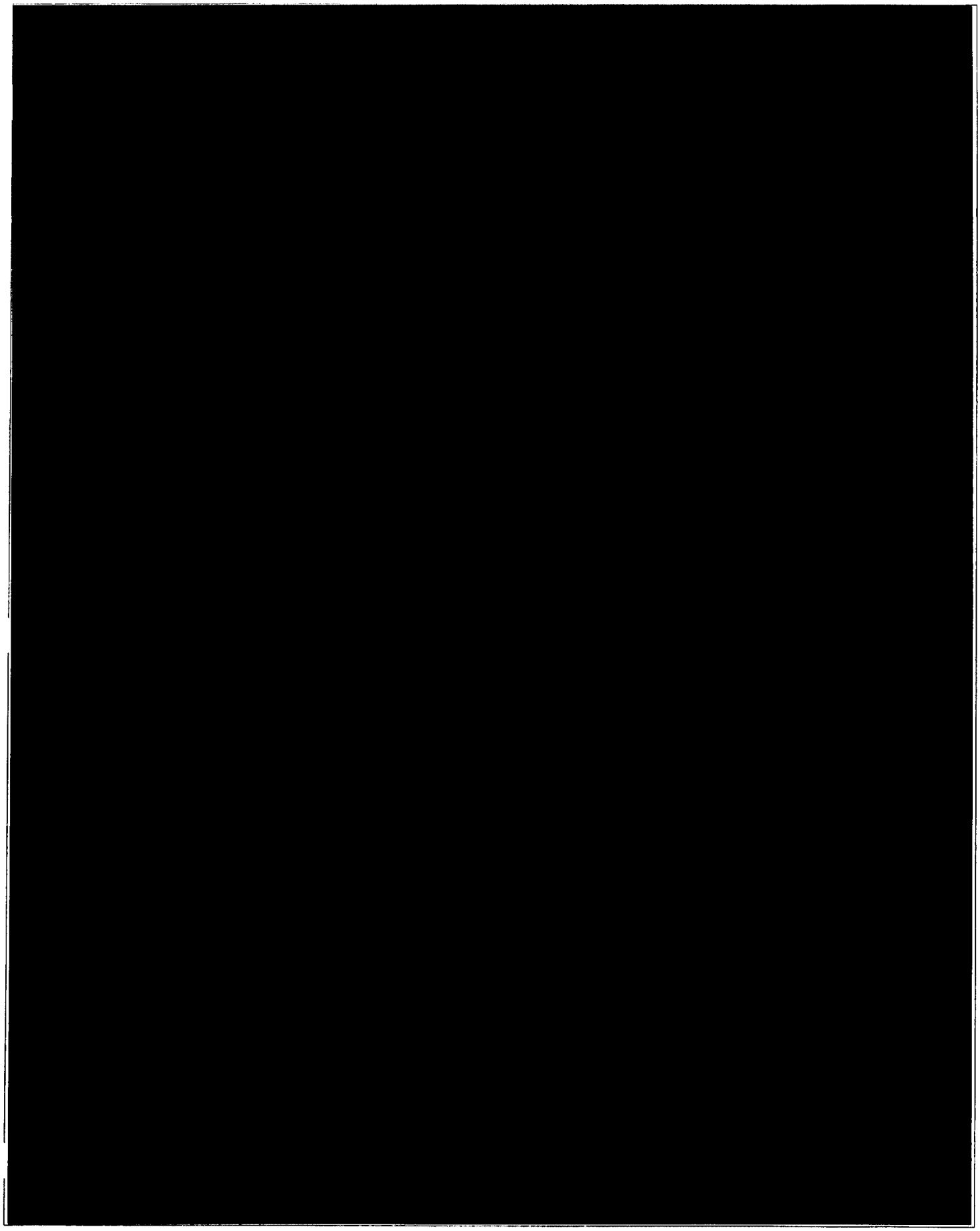
(1) Purpose of Interview: Gain an understanding of PEF's initiatives and policies concerning Data Security.

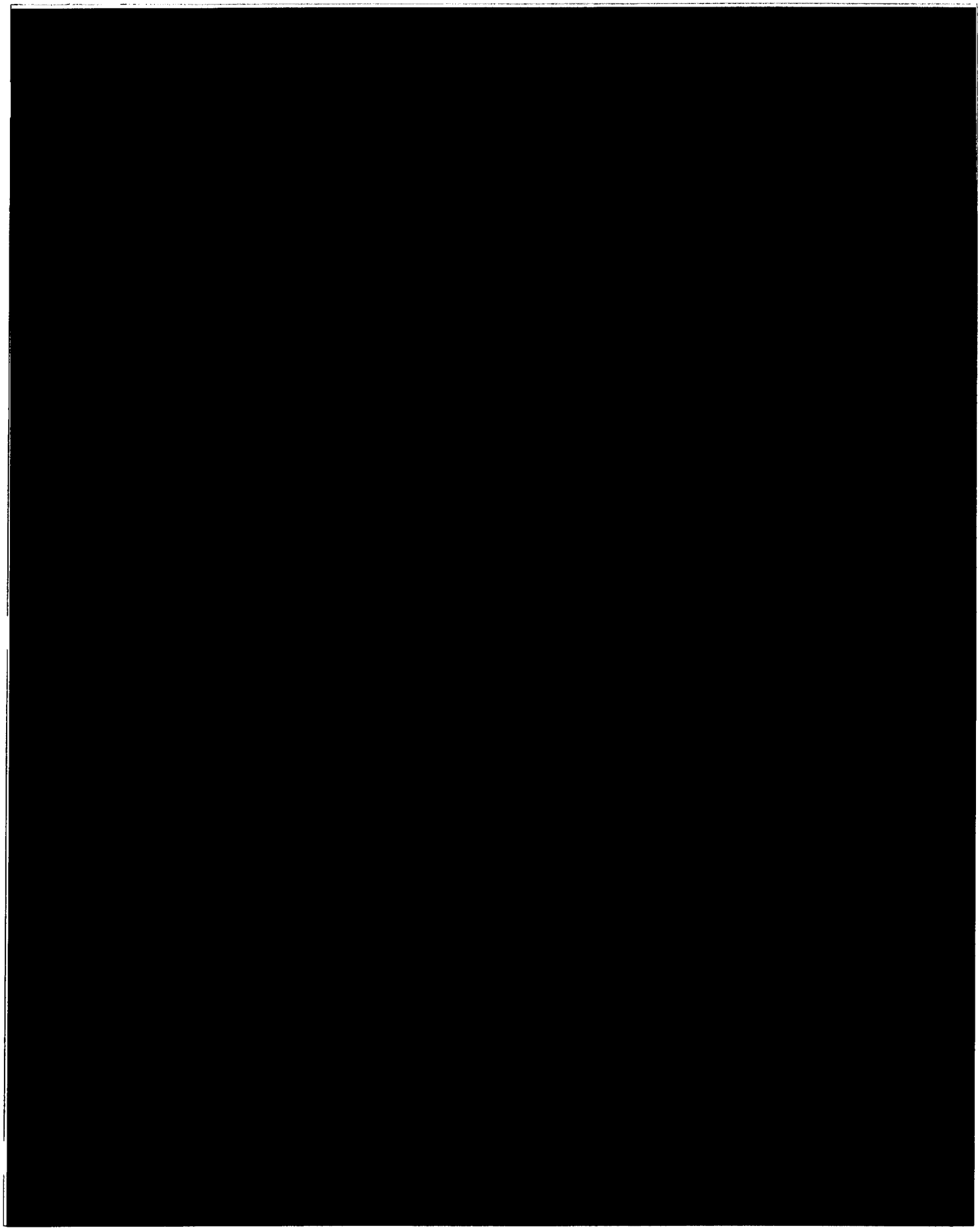
(2) Interview Summary:

[redacted]









[redacted]

(3) Conclusions:

(4) Date Request(s) Generated:
No. ____

(5) Follow-up Required:

Project Manager