FPL

November 26, 2014

-VIA HAND DELIVERY -

Carlotta Stauffer, Director
Division of Commission Clerk
Florida Public Service Commission
2540 Shumard Oak Blvd.
Tallahassee, FL 32399-0850

REDACTED

Re: Docket No. 140000
Florida Public Service Commission ("FPSC") Staff's Review of Physical Security Protection of Utility Substations and Control Centers

Dear Ms. Stauffer:

Enclosed for filing in the above described docket are an original and seven (7) copies of Florida Power & Light Company's ("FPL's") Request for Confidential Classification of FPSC Staff's report "Review of Physical Security Protection of Utility Substations and Control Centers" and Audit PA-14-05-003 Official Workpapers. The original includes Exhibits A, B (two copies), C and D. The seven copies do not include copies of the Exhibits.

Exhibit A consists of the confidential documents, and all information that FPL asserts is entitled to confidential treatment has been highlighted. Exhibit B is an edited version of Exhibit A, in which the information FPL asserts is confidential has been redacted. Exhibit C consists of FPL's justification table supporting its Request for Confidential Classification. Exhibit D contains two affidavits in support of FPL's Request for Confidential Classification. Also included in this filing is a compact disc containing FPL's Request for Confidential Classification and Exhibit C in Microsoft Word format.

Please contact me if there are any questions regarding this filing.

Sincerely,

David M. Lee
Fla. Bar No. 103152

COM	
AFD	1
APA	2 + CD + Redacted
ECO	1
ENG	1
GCL	1
IDM	1
TEL	
CLK	

Enclosures
cc: Carl S. Vinson
Sofi Delgado Perusquia

Florida Power & Light Company
David M. Lee, Senior Attorney
700 Universe Boulevard, Juno Beach, FL 33408-0420
Ph.: (561) 691-7263 Fax: (561) 691-7135

BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

Review of Physical Security Protection of Utility Substations and Control Centers	Docket No. 140000 Filed: November 26, 2014

REQUEST FOR CONFIDENTIAL CLASSIFICATION OF FLORIDA PUBLIC SERVICE COMMISSION STAFF'S REPORT AND OFFICIAL WORK PAPERS RELATED TO STAFF'S REVIEW OF PHYISCAL SECURITY PROTECTION OF UTILITY SUBSTATIONS AND CONTROL CENTERS

Pursuant to Section 366.093, Florida Statutes, and Rule 25-22.006, Florida Administrative Code, Florida Power & Light Company ("FPL") requests confidential classification of certain information included in the "Review of Physical Security Protection of Utility Substations and Control Centers" report (the "Report") and the Audit PA-14-05-003 Official Workpapers (the "Workpapers") prepared by the Florida Public Service Commission Office of Auditing and Performance Analysis. In support of its request, FPL states as follows:

1. Staff conducted an investigation regarding physical security of the transmission and distribution substations and control centers for Florida's investor owned utilities, including FPL. During its investigation, Staff was provided access to numerous pages of Confidential Data Responses, and FPL contemporaneously served notices of intent to seek confidential classification. Pursuant to Rule 25-22.006(3)(a), Florida Administrative Code, FPL was given until December 1, 2014[1], to file a formal request for confidential classification with respect to the Report and the Workpapers. Accordingly, FPL is filing this Request for Confidential Classification to maintain continued confidential handling of the information contained in the Report and the Workpapers.

[1] Commission Staff provided FPL a copy of the draft report on November 6, 2014. In the transmittal letter Staff indicated that due to the 21 day period ending on the Thanksgiving Holiday, FPL may file this request on December 1, 2014.

2. The following exhibits are included with and made a part of this request:

a. Exhibit A includes a copy the confidential Report and Workpapers, on which all information that is entitled to confidential treatment under Florida law has been highlighted.

b. Exhibit B consists of a copy of the confidential Report and Workpapers, on which all information that is entitled to confidential treatment has been redacted.

c. Exhibit C is a table containing the specific line, column or page references to the confidential information, and references to the specific statutory bases for the claim of confidentiality and to the affiant who supports of the requested confidential classification.

d. Exhibit D includes the affidavits of John Large and Mike C. O'Neil.

3. FPL submits that the highlighted information in Exhibit A is proprietary confidential business information within the meaning of Section 366.093(3), Florida Statutes. This information is intended to be and is treated by FPL as private in that the disclosure of the information would cause harm to customers or FPL's business operations, and its confidentiality has been maintained. Pursuant to Section 366.093, such information is entitled to confidential treatment and it is exempt from the disclosure provisions of the public records law. Thus, once the Commission determines that the information in question is proprietary confidential business information, the Commission is not required to engage in any further analysis or review such as weighing the harm of disclosure against the public interest in access to the information.

4. As the affidavits included in Exhibit D indicate, some of the information contained in the Report and the Workpapers is proprietary, confidential business information.

The Report and the Workpapers contain security measures, systems, or procedures, the disclosure of this which would jeopardize the safe operation of FPL's electrical system. Such information is protected by Section 366.093(3)(c), Florida Statutes.

5. Upon a finding by the Commission that the information highlighted in Exhibit A, and referenced in Exhibit C, is proprietary confidential business information, the information should not be declassified for a period of at least eighteen (18) months and should be returned to FPL as soon as the information is no longer necessary for the Commission to conduct its business. *See* § 366.093(4), Fla. Stat.

WHEREFORE, for the above and foregoing reasons, as more fully set forth in the supporting materials and affidavits included herewith, Florida Power & Light Company respectfully requests that its Request for Confidential Classification be granted

Respectfully submitted,

David M. Lee
Senior Attorney
Florida Power & Light Company
700 Universe Boulevard
Juno Beach, FL 33408
Telephone: (561) 691-7263
Facsimile: (561) 691-7135

By: _____
David M. Lee
Fla. Bar No. 103152

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing* FPL's Request for Confidential Classification Of Report And Workpapers Related To Staff's Review of Physical Security Protection of Utility Substations and Control Centers was served electronically via email this 26th day of November, 2014 to the following:

Carl S. Vinson
Sofi Delgado Perusquia
Florida Public Service Commission
2540 Shumard Oak Blvd
Tallahassee, Florida 32399-0850
cvinson@psc.state.fl.us
sdelgado@psc.state.fl.us

By: _____
David M. Lee
Fla. Bar No. 103152

*The exhibits to this Request are not included with the service copies, but copies of Exhibits B, C, and D are available upon request.

EXHIBIT A

CONFIDENTIAL

FILED UNDER SEPARATE COVER

EXHIBIT B

REDACTED COPIES

EXHIBIT B

CONFIDENTIAL

4.0 Florida Power & Light Company

4.1 Security Management

4.1.1 Security Organization

Florida Power and Light's (FPL) Corporate Security department is responsible for the security management of all non-Nuclear facilities. This includes those security issues related to substation and control centers. These responsibilities include the identification, assessment, and management of security risks, as well as the physical security of all FPL facilities. Corporate Security's physical security approach includes the following steps to prevent and mitigate attack:

- Deterrence and delay
- Detection of attack
- Assessment of attack
- Communication and notification
- Response to attack

Most Corporate Security personnel are former federal, state, and local law enforcement employees. FPL's Corporate Security department includes Area Security Managers responsible for geographical areas throughout FPL's service territory. They oversee the security of the facilities in their assigned areas and interact with local law enforcement. All Area Managers communicate internally and share law enforcement contacts and other pertinent information.

FPL states it remains vigilant of emerging threats. [redacted] FPL incorporates the use of contracted guards. Corporate Security determines the location of the guards based on the type and prioritization of the facility.

FPL's Corporate Security Department utilizes its Security Operations Center to monitor and manage all security threats. The Center is manned 24 hours every day and acts as a point of contact for police and employees if a security breach occurs. Personnel at the Center manage all security technology such as card readers and video surveillance. The Center also acts as the Disaster Recovery Center. Corporate Security personnel conduct all internal and external investigations dealing with FPL security.

Corporate Security uses an array of software to monitor physical security. [redacted]

Corporate Security personnel prepare a *Copper Theft Quarterly Report*, which tracks and trends thefts to see what additional measures may need to be implemented. These reports are reviewed by the Area Security Managers and the appropriate business units. As trends arise at certain substations, [redacted]

4.1.2 Physical Security Policies and Plans

FPL's *Enterprise Physical Security Plan* addresses the physical security of critical assets and their associated critical cyber assets as required by CIP-006. These are the assets identified as critical under current CIP Version 3 standards. With the implementation of Version 5 criteria, this set of assets will expand. The Physical Security Plan provides guidelines for the physical security of the FPL critical cyber assets within the substation control house. This plan is reviewed and updated annually.

NextEra's Compliance and Responsibility Organization provides independent oversight of compliance with the NERC standards across all NextEra subsidiaries including FPL. The Compliance and Responsibility Organization works with the operating Business Units such as Corporate Security and Power Delivery to ensure compliance with all NERC standards. Within FPL, each of the operating business unit's compliance teams ensure the execution of compliance activities, including the implementation and adherence to the company policies pertaining to NERC standards.

Additional FPL plans include the *Threat Level Response Plan* and the NextEra Energy *Cyber Security Incident Response Plan*. FPL's *Threat Level Response Plan* is comprised of general guidelines and potential protective measures suggested by the Department of Homeland Security. These guidelines would be implemented in conjunction with Business Unit procedures if the National Terrorism Advisory System Alert Level is raised. The *Cyber Security Incident Response Plan* covers the identification, classification, response, and reporting of incidents dealing with cyber assets. The plan provides general guidelines and team structure for appropriate company response. The Cyber Security Incident Response Team participates in annual tabletop exercises to test the effectiveness of the plan.

FPL suppliers and contractors must adhere to the *Supplier Safe and Secure Workplace Policy*. This policy outlines all requirements and procedures for working at FPL critical facilities such as enhanced background checks and drug testing.

4.1.3 Interactions with Law Enforcement and Federal Agencies

FPL uses local law enforcement to patrol substations and act as first responders to security related incidents. FPL Area Security Managers act as liaisons with local law enforcement of their assigned areas. FPL participates in the South Florida Regional Terrorism Task Force led by the West Palm Beach Sherriff's Department. Corporate Security is an active member of the Florida State Fusion Centers, which educate law enforcement about the critical assets across the state and share threat information. FPL is also an active member of the Secret Service led Miami Electronic Crime Task Force which focuses on cyber related crimes. It also has designated a central point of contact for federal agencies and local law enforcement. After the PG&E Metcalf attack, FPL began increasing local law enforcement training on substation equipment and incorporating first responders into emergency drills. FPL has also briefed law enforcement on the substations within their particular jurisdiction.

A B C D

FPL's Corporate Security maintains open communication channels with EEI's Security Committee and federal agencies such as a monthly ES-ISAC conference call that discusses security trends and best practices. FPL has also implemented its Security Notification and Event Reporting Procedure, which outlines the steps of event reporting to federal agencies in case of a security related incident involving control centers and substation facilities.[1] Under this requirement, FPL has reported [redacted] events in the years 2010 to 2014, none of which resulted in customer outages. Corporate Security also screens information from media, law enforcement, and federal agencies and disseminates it to upper management. FPL also participates in the following energy sector groups:

- Electricity Sector - Information Sharing and Analysis Center
- Industrial Control Systems- Cyber Emergency Response Team
- Edison Electric Institute
- Infraguard
- UNITE

FPL upper management is actively involved in interactions with federal agencies and sector groups. FPL plays a key role in the national EEI Security Committee, the FBI's National Joint Terrorism Task Force, and the Florida State Police Chief's Association.

4.1.4 Physical Security Cost Tracking

Corporate Security's budget encompasses both O&M and Capital components. O&M expenditures include the maintenance of existing physical security systems such as card readers, video surveillance, and intrusion detection. Capital expenditures include both new installations and life cycling of existing equipment. However, not all security costs are contained within the Corporate Security budget. Some physical security costs are shared with appropriate operational business units. For example, the cost of security equipment for new substations is rolled into the cost of the substation. Not all physical security costs are budgeted and tracked in separate line items. Therefore, difficulties exist estimating total costs of FPL's physical security efforts. Currently, FPL is exploring ways to capture future information that separately identifies physical security costs for control centers and substations.

FPL's Corporate Security budget is shown in **Exhibit 7** indicating an increase in spending for 2014 YTD. The increase in capital expenditures in 2014 is due to the end-of-life replacement of equipment, enhancements to existing sites, and new equipment at new sites.

Florida Power & Light Company
Corporate Security Budget
2011–2014

Year	Capital Expenditures	Operations and Maintenance	Total
2011	[redacted]	[redacted]	[redacted]
2012	[redacted]	[redacted]	[redacted]
2013	[redacted]	[redacted]	[redacted]
2014*	[redacted]	[redacted]	[redacted]

[1] NERC EOP 004-2 standard

*Through June 2014

Exhibit 6 *Source: Document Request Response 4-2*

4.2 Transmission Physical Security Protection

NERC CIP standards focus on the Bulk Electric System, which includes all transmission facilities that operate at 100kV and above. FPL operates 71 transmission substations and 47 combined[2] transmission and distribution substations throughout its service territory ranging from 100kV to 500kV. Security measures for transmission substations are tailored to each location based upon the individual facility needs, the criticality of the facility, and its unique location.

4.2.1 Risk and Vulnerability Assessments

Under CIP Version 3, transmission substations are classified as either critical or non-critical. All critical substations and transmission control centers, including back-up centers, are required to comply with NERC CIP standards. As required by CIP-002, Version 3, FPL developed a risk-based methodology to identify those transmission facilities which are critical to the reliability of the grid. Criticality is based on the potential impact the loss of a facility may have to the reliability of the FPL transmission system. Once a substation is deemed critical, their cyber assets are evaluated and protected based on their criticality to the reliability of the substation.

For facilities designated as *critical* for CIP compliance purposes, both the Physical Security Perimeter and the Electronic Security Perimeter of the cyber asset are highly safeguarded. The Physical Security Perimeter is the six-wall "barrier" (walls, ceiling, and floor) that houses the cyber asset. In most cases, the six-wall barrier is either the control center or the control house building at a substation. [redacted] and substations are required under CIP standards to employ security measures above FPL's baseline and may include additional measures such as [redacted] All critical and non-critical substations adhere to FPL's baseline security measures, which include a [redacted]

Additionally, the FPL business unit may deem a substation as a *non-critical priority substation* based upon the facility's history of security related incidents and increased theft patterns. Some of these priority substations receive Facility Security Reviews as well as additional security measures that critical CIP stations typically use.

Select transmission substations are protected with [redacted]

FPL has instituted Facility Security Reviews as vulnerability assessments and inspections for some transmission substations. FPL also ensures all transmission and

[2] Combined substations are sites that have both transmission and distribution substation in the same facility.

distribution substations meet all National Electrical Safety Code requirements for fencing, signage, and equipment. Procedures are updated every five years as the National Electrical Safety Code is updated.

FPL conducts Personnel Risk Assessments, or enhanced background checks, for employees and contractors to have unescorted access to critical facilities. Personnel Risk Assessments of some Corporate Security contractor employees are audited periodically by Corporate Security. FPL has the discretion to deny any contractor employee access to the critical facility for any reason. Under NERC CIP standards, all enhanced employee background checks must be conducted every seven years.

While FPL does not conduct formal risk or vulnerability assessments of its non–critical transmission substations, the company constantly monitors crime indices as well as incident trends to reassess its security protection. **Exhibit 8** shows the number of security incidents that occurred in its 71 transmission substations over the period 2010 to date. [redacted] is the most frequently occurring incident type.

Florida Power & Light Company
Transmission Substation Security Incidents
2011–2014

Types of Incidents	2011	2012	2013	2014*	Total
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

* Through September 2014

Exhibit 7

Source: Document Request Response 4-2

Exhibit 9 shows the number of security incidents that occurred in its 47 substations that have combined transmission and distribution operations. [redacted] Combination substations experienced an increase in the number of incidents in 2011. The number of incidents decreased in the subsequent years. [redacted]

Florida Power & Light Company
Combination Substation Security Incidents
2011–2014

Types of Incidents	2011	2012	2013	2014 *	Total
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

* Through September 2014

Exhibit 8

Source: Document Request Response 4-2

4.2.2 Physical Security Inspection Process

FPL's physical security inspections are the Facility Security Reviews. These reviews are performed at both critical substations and non-critical priority substations. These reviews evaluate [redacted] As required by CIP-006-03, reviews of critical facilities must be completed every three years. However, FPL typically performs them yearly or more often than the three year requirement. Facility Security Reviews are conducted by the Area Security Manager. The Manager reviews a security device inventory and previous Facility Security Reviews.

FPL's facilities management contractor also conducts facilities inspections of all critical and non-critical transmission substations five times a year. These facility inspections focus on the facility management and vegetation. They also incorporate a physical security component addressing doors, locks, fencing, and lighting.

4.3 Distribution Physical Security Protection

Distribution substations fall under the jurisdiction of the Public Service Commission as do transmission facilities below 100kV. The Bulk Electric System, including transmission substations, falls under the jurisdiction of FERC. Distribution substations connect to the transmission system, reduce the transmission voltage to 13 or 23kV, and terminate at a lower voltage below 1 kV at the customer's premise. FPL has 472 distribution substations throughout its service territory.

4.3.1 Risk and Vulnerability Assessments

FPL monitors security incident trends and crime indices to assess the risks faced by its various facilities. While FPL performs Facility Security Reviews at its distribution control centers, it does not perform documented risk or vulnerability assessments of its distribution substations. FPL ensures all substations meet all National Electric Safety Code requirements, such as specified fencing. Procedures are updated every five years as the National Electric Safety Code is updated.

All substations have FPL's baseline security measures, which include [redacted] An increase in security measures for distribution substations above the baseline, [redacted] is determined by analyzing crime trends and FPL's ongoing risk assessments.

FPL does not consider [redacted] Distribution substations serve a relatively small customer count and are often looped, providing for rapid rerouting and brief service interruptions. [redacted].

Exhibit 10 shows the recent numbers of security incidents that occurred in distribution substations. [redacted]

[redacted] are the least common types of incidents. However, [redacted] Overall, the number of incidents has decreased since 2011.

4.3.2 Physical Security Inspection Process

While FPL performs Facility Security Reviews at its distribution control centers, it does not conduct them for its distribution substations. However, it does conduct facilities inspections that incorporate physical security aspects. Like those for the transmission substations, these facility inspections are conducted by the facilities management contractor and are performed five times a year. These facility inspections address physical security components including [redacted]

Florida Power & Light Company
Distribution Substation Security Incidents
2011–2014

Types of Incidents	2011	2012	2013	2014 *	Total
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

* Through September 2014

Exhibit 9

Source: Document Request Response 4-1

4.4 Recovery And Response

FPL has implemented multiple levels of resiliency and redundancy in both its transmission and distribution substations and control centers. The primary transmission control center monitors the transmission grid and, among other roles, acts as the "generation to load" balancing agent for the company. The back-up control centers are geographically dispersed and are kept ready in case the primary control center losses functionality. The primary control center and the back-up centers are equipped with [redacted]

The control centers house the [redacted] One of these applications is the Contingency Analysis, which is performed every five minutes to assess the Bulk Electric System ramifications of losing one piece of FPL

equipment (e.g. transmission line). This allows the System Operator to see how FPL's infrastructure would handle an unexpected incident.

Since FPL is the FRCC Reliability Coordinator's agent, FPL's transmission control center also houses the FRCC Reliability Coordinator who are FPL shift employees whose responsibility is to monitor the FRCC regional footprint and to take any actions necessary to maintain the reliability of the Bulk Electric System consistent with NERC Reliability Standards. These employees observe the activity of all the utilities in the FRCC region and are required to resolve reliability issues between member utilities. Additionally, FPL participates in the FRCC Generating Capacity Plan adopted by the Commission per Rule 25-6.0183. The Generating Capacity Plan details the coordinated actions among electric utilities and state and local agencies. The FRCC plan enables FPL to cope with a generating capacity shortage on its system and to mitigate the impact of the emergency.

To build in resiliency and redundancy into FPL's transmission system, multiple lines may feed each substation, and substations typically house multiple transformers. If one transformer is inoperable, the other transformer(s) within the substation can typically accommodate the transferred power from the inoperable transformer. Spare equipment is also available for end-of-life replacement or to replace a damaged transformer. [redacted].

Beyond its own spare equipment supply, FPL participates in the EEI Spare Transformer Equipment Program (STEP), which allows utilities to find and share spare equipment in case of an emergency. FPL shares equipment in the 500/230 kV and 230/138 kV classes. Since the transport of these transformers can be an issue due to their size and need for specialized rail cars, this regional sharing arrangement can shortcut recovery time.

If an attack were to occur causing a transmission line to become inoperable, power is automatically rerouted minimizing the impact to the Bulk Electric System and customers. The System Operator at the transmission control center would monitor the Bulk Electric System to identify and respond to resulting adverse reliability conditions. [redacted] If that is also lost, alternate arrangements are implemented until communication is restored. Also, during the period when communication is unavailable, the substation and protection system equipment will still automatically respond and remedy fault conditions (e.g. tree coming in contact with a wire).

[redacted] These distribution control centers control and monitor all of FPL's distribution substation feeders. [redacted] even though they are not required to do so to comply with NERC CIP standards.

The distribution system is different from the transmission system in that it is a radial system. Feeders can connect to feeders from adjacent substations. Similar to most transmission substations, distribution substations can continue to function when one of the transformers is inoperable. For distribution substations with one transformer, feeders from the affected substation are typically reconnected to feeders from adjacent substations. Spare equipment is also available for end-of-life replacement or to replace a damaged transformer. [redacted] FPL also has the ability to deploy mobile transformers as needed when a distribution

substation transformer becomes inoperable. As another measure of redundancy protection, distribution substations are typically fed from multiple transmission line sections.

FPL's 590 transmission, combination, and distribution substations do not often experience complete substation outages. **Exhibit 11** shows the number of complete substation outages excluding planned outages and outages caused by named storms. These outages were caused by weather, equipment failure, and animals. None of the outages were caused by a malicious attack or physical security breach.

Florida Power & Light Company Transmission and Distribution Substation Unplanned Outages* 2011–2014	
Year	**Number of Outages**
2011	121
2012	93
2013	99
2014**	82
Total	**395**

* Excluding outages caused by named storms
** Through August 2014

Exhibit 10

Source: Document Request Response 3-8

4.5 CIP-014 Preparations

As a result of the PG&E Metcalf attack, FPL began conducting a series of self-assessments to gauge and improve its security measures. FERC developed a list of "electrically significant stations" that are vital to the reliability of the grid and a guideline of security measures which could be evaluated. FPL reviewed the list of FERC security measures and information from an EEI electric industry physical security survey in order to perform a "gap analysis" against FPL's current practice. FPL was able to identify potential enhancements at its high priority facilities. An EEI working group was able to use these results to benchmark current practices within the electric sector. Corporate Security also utilized the Department of Homeland Security's Computer Based Assessment Tool, a vulnerability assessment of critical assets to create a video guide of five facilities. Corporate Security utilized this video-guide to increase situational awareness of select substations for the Security Operations Center personnel.

From the gap analysis conducted, multiple potential security enhancements for transmission substations were identified. Some of these enhancements include:

[redacted]

[redacted]

Some of these enhancements have been implemented while others have been delayed for comparison to the eventual final CIP-014 requirements.

FPL actively participated in the drafting and development of CIP-014. A member of the NextEra Compliance and Responsibility Organization served as the Chairman of the NERC Standards Committee, which oversees and manages the development of the CIP-014 standard. An FPL Power Delivery employee was a member of the drafting team which developed and wrote the CIP-014 standard. Although the final version of CIP-014 has not been approved by FERC, FPL has begun to identify the substations that will be applicable under CIP-014. The new standard will encompass a smaller subset of substations derived from the medium impact category under CIP Version 5. FPL will be required to assess medium impact substations to determine their effect on the reliability of the grid. FPL states that no major planning or cost projections can be prudently developed until FERC approves the CIP-014 standard.

4.6 Self-Assessments And Exercises

FPL participated in the GridEx II exercise in 2013, in a monitor and respond role. Key NextEra Energy business units participated in the exercise. After the completion of the exercise, NextEra Energy identified certain needed areas of improvement. NextEra Energy and FPL plan to participate as active participants in the GridEx III exercise in November 2015.

The Enterprise Physical Security Plan required by CIP-006-03 is tested yearly via tabletop exercises which simulate the recovery of critical systems (CIP-009) and incident response procedures (CIP-002). FPL personnel act as both the participants and facilitators in the exercise. Third party contractors have facilitated the exercises in the past. NextEra Energy also conducts annual, cross-departmental cyber threat exercises that sometimes include physical security scenarios. The cyber drills are conducted and facilitated by the cyber team and Corporate Security and have been monitored by federal agencies such as the FBI.

4.7 Company Comments

Office of Auditing and Performance Analysis
Document Summary and Control Log

Company: Florida Power & Light
Area: Physical Security of Substations
Auditor(s): Delgado Perusquia/Coston

Workload Control #: PA-14-05-003
File Name: I:\PERFORMANCE ANALYSIS SECTION\00 PERFORMANCE ANALYSIS AUDITS\Physical Security\FPL\3.0 Work Papers\3.3 Document Summaries\3.3.1 Document Summary.doc

Document #: 1-1
Date Requested:
Date Received:
Comments: (i.e., Confidential)

CONFIDENTIAL

Document Title and Purpose of Review: a. Does your company have a physical security policy, strategy or governing document? **b.** Describe how this physical security policy is reviewed or audited. **c.** If so, how often reviews and audits are performed? **d.** Is the review or audit conducted internally or by an outside party? **e.** What qualifications does the company consider relevant to this type of review?

Summary of Contents: a. [redacted] They also adhere to the National Electric Safety Code, Section 11.
b. CIP-006-3 and EOP-004-2 are reviewed by FPL personnel. Audits are also performed by FRCC.
c. CIP-006-3 and EOP-004-2 reviews are done annually, and the FRCC audits are conducted every 3 years.
d. Both (Internally and by a 3rd party)
e.

Conclusions:

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

Follow-up Required:
1. Please refer to FPL's response to document request, question 1-1(b), which FPL personnel review CIP-006-3 and EOP-004-2? Please describe their job responsibilities.
2. Who id the 3rd party that performs the reviews?
3. Please describe how the reviews are recorded.
4. Please provide the Enterprise Physical Security Plan and the Security Notification and Event-Reporting Procedure.
5. Please provide any documentation of the most recent review of CIP-006-3 and EOP-004-2 performed by FPL personnel.
6. Please provide the most recent audit report performed by FRCC.

Document #: 1-2
Date Requested:
Date Received:
Comments: (i.e., Confidential)

Document Title and Purpose of Review: a. Has your organization conducted a physical risk or vulnerability assessment of its transmission substations, distribution substations, and system control room facilities? **b.** How were these assessments conducted? **c.** Who conducted these assessments? d. How often are these assessments revisited or redone?

Summary of Contents: a. Yes, for those substations and control centers identified as critical by the company.
b. Via on-site reviews of physical security such as lighting, fencing, access control devices, locking mechanisms, video surveillance, signage and with frequent law enforcement liaisons.
c. FPL Area Security Managers.
d. The assessments are performed annually or every six months based on criticality of the substation or control center facilities.

Conclusions:

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

Follow-up Required:

1 2 3 4 5 6 7 8 9 10 11 12 13 14

	1. Please refer to FPL's response to document request, question 1-2(b), how do the FPL Area Security Managers conduct a physical risk or vulnerability assessment of its transmission substations, distribution substations, and system control room facilities? What processes and criteria do they use to conduct these assessments? 2. Please provide any documentation of the most recent review. 3. Please provide all of the dates for the on-site reviews conducted of the transmission substations, distribution substations, and system control room facilities for 2012, 2013, and year-to-date 2014. 4. Please describe the job responsibilities of the FPL Area Security Managers. 5. Please refer to FPL's response to document request, question 1-2(c), how does FPL assign criticality of substations or control center facilities? Please provide any standards or documentation related to assigning criticality.
Document #: 1-3 **Date Requested:** **Date Received:** **Comments: (i.e., Confidential)** 3(a) CONFIDENTIAL	**Document Title and Purpose of Review: a.** Has your physical security plan been reviewed in the last year and updated as needed? **b.** How often is it reviewed and updated?
	Summary of Contents: a. CIP-006-3 – [redacted] EOP-004-2 – [redacted] NESC (every 5 years by Institute of Electrical and Electronic Engineering) reviewed by FPL to determine if changes to policies sand procedures are required. Last review in 2012. **b.** Please see FPL's response to Staff's First Data Request No. 1.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1.
Document #: 1-4 **Date Requested:** **Date Received:** **Comments: (i.e., Confidential)** 4(a) CONFIDENTIAL	**Document Title and Purpose of Review: a.** Is your physical security plan tested regularly? **b.** Is it tested internally or by or with a third party? **c.** How often is it tested?
	Summary of Contents: a. CIP-006-3 is tested annually. **b.** Both (Internally and by a 3rd party) **c.** See FPL's response to subpart (a) above.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. Please refer to FPL's responses to document request, question 1-4(b), what part of your organization tests your physical security plan? Please describe their job responsibilities. 2. Please refer to FPL's responses to document request, question 1-4(a), describe how your organization tests Enterprise Physical Security Plan (CIP-006-3)? What roles do FPL's personnel and the third party contractors play in the testing? 3. Who is the 3rd party?
Document #: 1-5 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)**	**Document Title and Purpose of Review:** How does your physical security plan identify critical assets?
	Summary of Contents: The Enterprise Physical Security Plan for NERC Standard CIP-006-3 does not specifically identify critical assets. However, FPL does identify critical substation and control center assets through application of a formal risk based methodology developed by FPL as required in the current NERC CIP-002 standard.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:

	Follow-up Required: 1. Has FPL developed a risk based methodology similar to the requirements in the current NERC CIP-002 standard for transmission facilities below 300KV as well as distribution substations? If so, please describe.
Document #: 1-6 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)** 6(c) CONFIDENTIAL	**Document Title and Purpose of Review: a.** How does your physical security plan include recognition of critical facilities and/or physical assets that are dependent upon IT or automated processing? **b.** How are interdependent service providers (for example, fuel suppliers, telecommunications providers, other outside vendors) included in risk assessments? **c.** How does your physical security plan include alternative methods for meeting critical functional responsibilities in the absence of IT or communication technology?
	Summary of Contents: a. See FPL's response to Staff's First Data Request No. 5. **b.** Interdependent service providers affecting critical facilities would be reviewed as part of the Facility Security Review process. **c.** In the absence of electronic information from one of the substations, the main critical functional responsibility of isolating electric components for a fault (electrical ground) condition is still performed automatically by the protection devices at the substation. FPL uses separate and diverse communication and data paths. Geographically diverse back-up control centers are used to add levels of redundancy. In absence, [redacted]
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. Please refer to FPL's response to document request, question 1-6(b), how are Facility Security Reviews documented? 2. Please provide the most recent Facility Security Review. 3. Please refer to FPL's response to document request, question 1-6(c), describe FPL's electric system footprint. 4. Please provide FPL's Loss of Control Center Functionality Plan. 5. 1-6(b), please point out where the independent service providers are included in the FSRs provided to us? 6. 1-6(c), describe FPL's electric system footprint. 7. Walk through of 6c scenario. 8. Explain what absence of electronic information entails? 9. How is law enforcement used in absence of IT/ communication? 10. Have you ever thought about having your own internal communications system instead of relying on an external interdependent carrier? 11. Please describe "still performed automatically by the protection devices at the substation"? 12. Please describe "voice communication"? 13. Describe "diverse communication and data paths"?
Document #: 1-7 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)**	**Document Title and Purpose of Review: a.** Please describe your interactions with the Department of Homeland Security, FERC, Department of Energy, FBI or other federal agencies regarding assistance with or cooperation in physical security. **b.** Has your company conducted a physical security evaluation of key assets in concert with the Department of Homeland Security or other federal agencies? Please describe. **c.** Has your company conducted a physical or cybersecurity program maturity model assessment on its own or in cooperation with any federal agency? (For example, C2M2 FERC assessment) Please describe.
	Summary of Contents: a. FPL routinely communicates with governmental agencies such as the Joint Terrorist Task Force (JTTF), FBI Domestic Security Advisory Committee (DSAC), Secret Service, Department of Homeland Security - Protective Security Advisors (DHS-PSA), and the Regional Domestic Security Task Force. FPL's interactions with these entities are not limited to

Date Requested: 11/22/10 **Date Received: 12/7/10** **Comments: (i.e., Confidential)**	(such as ES-ISAC, industry associations, etc.) to improve its physical security protections and readiness.
	Summary of Contents: We are members of organizations such as the Edison Electric Institute (EEI), EEI Security Committee, ES-ISAC, North American Transmission Forum (NATF) Physical Security Group, American Society for Industrial Security (ASIS) and the FBI Domestic Security Advisory Committee. A member of the Corporate Security department is the current Chairman of the national EEI Security Committee. The EEI Security committee has taken a lead role in the industry in the sharing of best physical security practices. FPL is investing in new physical security technology and is bench-marking with our peers to help ensure we are utilizing the best available physical security measures.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. What new technology are you investing in? 2. How is bench-marking performed?
Document #: 1-18 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)**	**Document Title and Purpose of Review: a.** Can your company identify any other mandatory physical security standards that apply to its systems? **b.** What is your company's plan for certifying its compliance or identifying that it has a timetable for compliance?
	Summary of Contents: a. No. While CIP-006 includes mandatory physical security requirements, these are limited to critical cyber assets/systems. **b.** As mentioned in FPL's response to Staff's First Data Request No. 16, FPL is working to be compliant with version 5 of CIP-002 through CIP-009 by the effective date of April 1, 2016 for High and Medium impact assets, and April 1, 2017 for Low impact assets. FPL's Compliance and Responsibility Organization will oversee these compliance activities to ensure compliance with version 5 by the required dates.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required:
Document #: 1-19 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)** CONFIDENTIAL	**Document Title and Purpose of Review:** Please describe any other pro-active physical security initiatives by your company that go beyond regulatory or standard compliance activities.
	Summary of Contents: FPL conducts FSRs more frequently than required (CIP-006-3). FPL networks on a frequent basis w/ Florida State Fusion Center and local/federal law enforcement on trends and threats affecting our sector. [redacted]
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. What is "frequent basis"? 2. Are there any specific sector groups just for physical security? 3. Please refer to FPL's response to document request, question 1-19, what is the role of the commercial intelligence vendor?
Document #: 1-20 **Date Requested: 11/22/10**	**Document Title and Purpose of Review:** How do you determine which systems, components, and functions get priority in regard to implementation of new physical security measures?

	detection system for the facility, and also reviewing the lighting, fence perimeter, video and other related security measures. In addition, all transmission and distribution employees while at a transmission or distribution substation for normal work activities will inspect these facilities for unlocked gates, damaged fencing, and other security/safety related issues. These same employees are provided training on reporting security related events through training courses related to Security Notifications and Event Reporting. (EOP-004-2) b. Please see Attachment Nos. 2 & 3 for the FSRs for a system control center and transmission substation respectively. At this time, we have not conducted any on-site reviews of Distribution Substations.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. Is there any review of physical security for distribution substations? 2. Why do some substations have more than one completed in a year? 3. Done at all control centers? 4. If there is an issue or finding found, how is it addressed? Re-audit? 5. Whose responsibility is it? 6. Is this a critical substation? 7. Go over recommendations. 8. Has this been corrected?
Document #: 2-6 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)**	**Document Title and Purpose of Review:** Please describe how FPL tests the Enterprise Physical Security Plan as referred to in response to question 1-4(a). What roles do FPL's personnel and the third party contractors play in the testing?
	Summary of Contents: The Enterprise Physical Security Plan for NERC Standard CIP-006-3 is tested by the utilization of tabletop exercises which simulate the recovery of critical systems and incident response procedures. FPL personnel act as both participants in the exercise and have facilitated the exercise. Third party contractors have also facilitated these exercises in the past.
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. Who are these third party contractors?
Document #: 2-7 **Date Requested: 11/22/10** **Date Received: 12/7/10** **Comments: (i.e., Confidential)** CONFIDENTIAL	**Document Title and Purpose of Review:** a. Please describe how the Facility Security Reviews referred to in response to question 1-6(b) are documented. b. Please provide the most recent Facility Security Review.
	Summary of Contents: a. The Facility Security Reviews (FSR) are documented in an [redacted] b. Please see FPL's response to Staff's Second Data Request No. 5(b).
	Conclusions:
	Data Request(s) Generated: No. _____ Description: No. _____ Description:
	Follow-up Required: 1. Describe the Investigative Database. 2. Who has access to it?

Office of Auditing and Performance Analysis
Document Summary and Control Log

Company: Florida Power & Light
Area: Physical Security of Substations
Auditor(s): Delgado Perusquia/Coston

Workload Control #: PA-14-05-003
File Name: I:\PERFORMANCE ANALYSIS SECTION\00 PERFORMANCE ANALYSIS AUDITS\Physical Security\FPL\3.0 Work Papers\3.3 Document Summaries\3.3.4 Document Summary 4.doc

Document #: 4-1
Date Requested:
Date Received:
Comments: (i.e., Confidential)

CONFIDENTIAL

Document Title and Purpose of Review: **a.** For distribution substations and control centers, please provide a count of incidents involving attempted intrusion of the fenced perimeter or buildings, theft, destruction of equipment/property, or vandalism. **b.** If presently readily available, provide a brief description of each event. (E.g. "2 suspects attempted to cut perimeter chain link fence but did not enter facilities" or "Theft of copper from company vehicle within substation fence.") **c.** Please provide this information separately by year for 2011, 2012, 2013 and YTD as available for 2014, noting cutoff date.

Summary of Contents:
a. Attachment Nos. 1 - 4 contain the list of all such incidents for the years 2011 through September 18, 2014, including distribution and transmission facilities.
b. Please see Attachment Nos. 1 - 4. The "Summary" of the Incident and "Case Type" provided in the attachment are preliminary information utilized by the Security Operations Center to classify and/or summarize the initial report of the incident. The subsequent investigation and/or follow-up may vary from these classifications based upon the facts/information that is discovered. FPL could not provide further detail in the limited time provided to respond to this data request.
c. Please see Attachment Nos. 1 - 4.

[redacted]

Conclusions:

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

Follow-up Required:

Document #: 4-2
Date Requested:
Date Received:
Comments: (i.e., Confidential)

CONFIDENTIAL

Document Title and Purpose of Review: **a.** For transmission substations and control centers, please provide a count of incidents involving attempted intrusion of the fenced perimeter or buildings, theft, destruction of equipment/property, or vandalism. **b.** If presently readily available, provide a brief description of each event. (e.g. "2 suspects attempted to cut perimeter chain link fence but did not enter facilities" or "Theft of copper from company vehicle within substation fence.") **c.** Please provide this information separately by year for 2011, 2012, 2013 and YTD as available for 2014, noting cutoff date.

Summary of Contents:
a. Please see FPL's response to Staff's Fourth Data Request No. 1.
b. Please FPL's response to Staff's Fourth Data Request No. 1.

c. Please FPL's response to Staff's Fourth Data Request No. 1.

Transmission

	2011	2012	2013	2014
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Conclusions:

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

Follow-up Required:

Document #: 4-3
Date Requested:
Date Received:
Comments: (i.e., Confidential)

Document Title and Purpose of Review: a. Please provide the total number of transmission substations. **b.** Please provide the total number of distribution substations.

Summary of Contents:
a. 71 transmission substations;
b. 472 distribution substations; and
c. 47 "combined" transmission and distribution substations

Conclusions:

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

Follow-up Required:

- Jim is on the Board of Directors
- Several people in Corporate Security have secret clearance
  - Needed for DOE briefings
    - Discuss trends and best practices
    - Other utilities share info
- Sr. Manager know sheriffs in FPL territory
- [redacted]
- Corporate Security Structure
  - 5 Security Managers are divided by geographical locations
    - Responsible for maintaining contact with law enforcement
    - **Law enforcement calls Security Center first**
  - Use a SharePoint site that contains contacts
  - If an attack happens, they call the security center
- Substation and Control Center Infrastructure
  - TCC and Transmission
    - 500-69 KV
    - Within the region, monitor transmission grid
    - Facilities
      - Redundancy when building power supply
      - Interim provision control center
      - Geographically diverse
    - Computer system
      - EMS fail to backup
    - Voice Communication
      - Fully redundant voice recording
      - Hoot & Holler system connected both internally and externally
      - Corporate phone system
      - Satellite phones
    - Real-time Data links to external entities
    - Reliability tools
      - Contingency analysis performed every 5 minutes
        - Looking at grid
        - Let operator know if there is a problem
        - Analysis of blackouts
        - Done regionally (FRCC)
    - Regional footprint

- Most of FL except panhandle
- FRCC
- Ratings
- Convert the power system into a big connected info structure

- Geographically diverse back up centers
- Primary CC
- Don't have to get everyone up to back-up
  - Not mapped
  - Have people there just in case not manned 24/7
- Interim Control Centers
- Substation Infrastructure
  - Auto transformers
  - Transmission: receive 230 KV -> 138KV
  - Distribution: 138KV -> 13.8KV

- DCC and Distribution
  - 23-13.8 KV
  - Monitors distribution substation feeders
  - Distribution [redacted]
    - Manned all the time

- NERC History
  - 2003 blackout triggered 2005 Energy Policy Act
  - **100 KV or larger is considered BES**
  - does not treat Transmission 69KV any differently
- Challenges
  - Human error
  - Op threat
  - Emergencies
  - Lack of preventative maintenance
- Protective devices
  - Like a circuit breaker
  - Protecting from fault that causes fire
  - Relays
    - Small electronics
    - Taking info that's there
- Training Personnel
  - Communication
- Prevent cyber intrusion
- **FRCC**
  - **Reliability Coordinator**
    - Monitoring regional footprint
    - Transmission coordinator
    - Overrides the utilities if needed
    - Inter-regional
    - Individual utilities control the equipment
    - Oversees the operation of the interconnection
- **CIP**
  - 2008 – Control Centers
  - 2010 – Critical infrastructure and control centers
  - Version 3
    - Cyber assets determined by a risk-based methodology
    - Rule-based method for cyber assets
  - Physical Security Perimeter
    - Cube
  - Electronic Security Perimeter

- Fire walls
- Defense in depth
- Internet ‖ Information management (#1) ‖ ‖ (#2) ‖ (#3) ‖ EMS (#4)
- Control Centers do not have email available on computers
- No trust between levels

- CIP Version 5.
  - 2016 and 2017 implementation
  - Bright line Criteria- more defined
  - **High** (CC)
  - **Medium** (priority transmission and plant sites)
    - [redacted]
  - **Low** (balance of transmission subs)
  - No prioritization within CIP or in terms of physical and cyber security
  - Methodology was looking in-house.
  - New plan must look at entire grid
- CIP -014
  - Director participated in team
  - Risk-assessment on critical assets
  - 3rd party verifier (agencies, utilities, consultants)
  - Threat and vulnerability assessment
  - Medium priority from v. 5 would be included
  - 3rd party review of evaluation and security plan
- Current Physical Security Practices
  - [redacted]
- **Metcalf**
  - Attack on Bank of transformers
  - The grid remained intact
    - No customer impact
  - Industry responded quickly to self-assessment
  - NERC assembled team of members to assess consistence of standards
  - Pre-Metcalf
  - Piloting outside-in system
  - [redacted]
- **Critical may be different from "electrically significant" substations**
- Substation Resiliency
  - Spare substation equipment is available; replacement or End Of Life
  - Mobile substation equipment is used (transformers, circuit breakers)
- STEP Connect
  - Participates in 500/230 KV and 230/138 KV classes
  - Enhancements
    - Cover generator step up (GSU's) and long-lead ancillary equipment
  - Continue to work with industry effects (EEI) on improved transportation
  - Transportation is currently a challenge
- Chairman of NERC Standards Committee

        - 2 PUCs helped (Nevada and Ohio)
        - all NERC standards have to go through committee
        - FERC started the process but cannot write the standards
        - NERC who implements the standards
        - Industry very receptive. They were already doing a lot of this.
        - Committee appointed technical team.
        - They committee, NERC, and the technical team were comfortable that they were covering the order.
        - BM met with FERC staff and believes there will be tweaks in the Thursday FERC order.
        - Next step would be FERC asking NERC questions within 30 days.
        - Trade associations will comment
        - Hopes FERC will have a final order in late fall (Nov or Dec)
        - Duke and Southern had people represented as well as munis and FRCC
        - Well represented in voting
        - FPL has 18 month period
        - Applies to medium risk (if removed, what would happen to grid)
        - Threat assessment
        - Some utilities will have no medium substations
        - Assessment will become very confidential
            - Review on site
        - Things in document that would keep things confidential
        - Push back
            - Foundation for … thought that CIP-014 was being too conservative (more in bucket than necessary)
- (2-12) security guard
    - [redacted] few based on theft
    - Time varies by location
- CBAT
    - 5 – substations
    - Use for security operations center
- [redacted]
- EEI physical security survey
    - industry benchmarking
- Leads on industry peers
    - Yard perimeter fencing
    - Lighting
    - Signage
    - Procedures
    - Intrusion detection and video surveillance
- **Enhancements considered**
    - [redacted]
    - local law enforcement and DHS
    - emergency dry runs were conducted with law enforcement
        - enhanced training EOP-004 (security reporting)
        - available to all employees
- Evaluate new technology
    - Spare equipment
- [redacted]

[redacted]

- GridEX II
  - NERC
  - 215 organizations (utilities, DHS, DOE, FBI, EEI, etc.)
  - Identify improvements in physical and cyber security attacks
  - Information from DC to groups
  - "monitor/respond" role
  - Helped NERC put exercise together
  - 2015 active participants
  - 70 people involved at control center
  - Key NEE deps were present
  - 1.5 days
  - Phishing
  - Shooting, explosions (war-like)
  - Realized FPL would need outside help if all this happened
  - Tested the plan
  - Lesson Learned on presentation
  - Network segregation
- Participation in future Physical/Cyber Exercises
  - Cyber drills with in
  - At least annually
  - FBI cyber person present at drill
  - Secret service
- "Air Gapping" control system networks
  - Levels with firewalls and physically separate
  - Communication one-way (dial)
- Beyond industry standard
- C2M2
  - Will have a reassessment this year
  - In fall other assessment 3rd party
  - Self-assessment or have DOE do it
  - Benchmarking b/w different utilities
  - Review with management
  - DOE Risk Management Process
- Threat Scenario Project – EEI Resiliency Self-Assessment
- Threat- Cyber Threat Intelligence (CTI)
- Situation
  - Qradar
  - Create Common Operational Picture
- Sharing
  - CTI
- NIST Framework
  - More smaller and midsize organizations
- No maturity model for physical
- ES-ISAC
  - NER run
  - cyber
- No CICC (?) #13
- Timeline for some
- UNITE
  - Benchmarking organization for electric

- Tiered approach to physical
- Tier system
  - BU determines criticality of substations
  - Primarily transmission substations
  - Going to see standards
  - Model to how affect
- No timetable for gap analysis
- CIP-014 implementations
  - Corporate Security and Business Units
  - Checked by CIP group

- 1-13
  - Law enforcement
  - Are security Managers might go out to look out there
  - Long-term
- 1-14
  - EMS all applications that the … used to monitor and control BES
  - More than 100 apps in EMS
- 1-17
  - EEI Security committee
  - Convened call with counterparts
  - Informal survey within committee
  - Creating contacts
- 1-19
  - [redacted]
  - 24/7 open source monitoring
  - [redacted]
  - Daily report
  - Primarily physical security threats
  - Other vendor "Critical Intelligence"
  - People report
  - Great preventative measure
- 1-23
  - Blocked 3rd party employees. Rejected.
  - Vendor does the background check
    - Audited quarterly last year
    - Now annually
- 1-24
  - Unescorted vendors
    - PRA
    - Training annually
    - Used for replacing cameras, repairing turnstile gate…
    - Only for the PSP of cyber assets
  - Escorted vendors
- 1-26
  - Organizational chart
  - Director
  - Administrative support
  - Security Managers (4)
  - Sr. Area Security
  - Sr. Manager Corporate Security
- 1-27
  - Industry certification by ASIS
    - Annual renewal
  - New employee training

- Not required but do it for…
- 2-2 (1)
  - Scope is 3 years in past (gap)
  - Difference of opinion
  - FRCC agent for NERC
  - Difference of opinion
  - NERC auditing handbook and training
    - Auditor training in fall
    - Full program will be implemented in 2016
    - There have been a couple of pilot programs in regions (SERC)
- 2-2 (2)
  - Routers open communications
  - Technology comes this way (open) rather than closed
  - Not documented correctly (vendor)
  - All findings are contested at the same time
  - Fines
    - Pro-rated
    - Come in from NERC but part of the budget of FRCC
  - If fixed, no fine
    - Risk-based
    - Small penalty $10K-$25K
- 2-2 (3)
  - Technology difference
  - Did them because they used proxy
  - Next audit in 2016
- 2-4
  - Non-critical
  - Distribution substations not target
    - Still expensive
  - Mostly theft
  - No cost-benefit analysis
  - Internal investigative database. Quarterly report
    - Publish report on copper theft
  - Need-basis security (incident driven)
  - Baseline of security
    - [redacted]
  - **FSR for critical transmission**
  - Gap repaired right away if poses threat
  - No formal procedure for critical issues
- 2-6
  - CIP-008
  - Exercise
    - BUs participate
  - Write concerns
  - Tabletop exercises
  - Done internally
  - Not sure when the next one will be

- 2-7
  - Investigative Database
  - Internal
  - Track incidents and investigations
  - Burglaries, thefts
  - Secure server
  - Redundant server
  - Security managers and other personnel have access by levels
- 2-8
  - Moving to corporate procedures
- 2-9
  - One non-critical
  - Access road to lines
  - FSR
  - Limited resources for physical security
- 2-12
  - [redacted]
  - Training for SOC personnel about critical equipment
    - Situational awareness
  - CBAT as a response for personnel
  - #4 EOP-004-Notification
  - No additional security
  - #7 redundancies for security infrastructure
  - Corporate Security or BU capital expense
  - How decide who pays
  - Sr. management within BU
- 2-13
  - Internal guide for BU guidance
  - Guidelines
    - Generally accepted guidelines created by DHS
  - Pg. 11 created by DHS
  - Is threat is increased, push out to Bus
  - Bus may or may not have procedures for increased threat level
- 2-14
  - Reports to Intelligence Analyst, John, and Director
  - Only M-F
- 2-15
  - No audits of random testing
  - Contractors who have badges, PRA and are frequent
  - Escorts at NERC CIP sites

(3) Conclusions:

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

(5) Follow-up Required:

        - Transfer
        - Can run on -1
        - Stations serve by 2 different transmission lines
        - Many have auto switches that could tie feeders together. Not everywhere
    - Resiliency
        - Spare equipment
- Distribution inspections
    - In addition to visits
    - Facilities management group do go out and assess
    - More than once a year
    - Fences, locks, perimeter, ground, building
    - For distribution and transmission
    - Electronic inspection
    - Done by contractor
    - Reviewed by area substation management
    - Work order
    - Tracked until completed
- Camera and equipment by vendor
    - Non-functional camera alert
    - Checked weekly
- Cyber drills
    - Jeff's team
- CIP v.5
    - Approved
    - April 2016
    - Teams interpreting standards
    - Policy and procedure link-up
    - Medium – similar to now CIP substations
    - Low – much larger figure
    - CIP not clear what the enhancements will be
- CIP-014
    - Stations that have large impact on grid
    - Looking at medium substations
    - Assessment of loss of substation on grid
    - Severe impact
    - This CIP will impact very few # of substations
- [redacted]

(3) Conclusions:

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

(5) Follow-up Required:

EXHIBIT C

JUSTIFICATION TABLE

EXHIBIT C

COMPANY: Florida Power & Light Company
TITLE: List of Confidential Documents
AUDIT REVIEW TITLE: Review of Physical Security Protection of Utility Substations and Control Centers
DATE: November 26, 2014

Description	Page Number	Conf. Y/N	Line/Column	366.093(3) F.S.	Affiant
Audit Report Section 4.0	1	Y	Lines 19-20	(c)	John Large
	1		Lines 29-38		Mike O'Neil
	2		Lines 4-5		Mike O'Neil
	3		Line 6		Mike O'Neil
	3		Lines 38-41, Col. B-D		Mike O'Neil and John Large
	4		Lines 22, 24, 25-27		John Large
	4		Lines 32-37		Mike O'Neil
	5		Lines 13-14, 19-24, 28-29		Mike O'Neil
	5		Lines 31, 36-38		Mike O'Neil
	6		Lines 1-3		Mike O'Neil
	6		Lines 9-10, 32-35		John Large
	6		Lines 37-38, 40, 42		Mike O'Neil
	7		Lines 1-3		Mike O'Neil
	7		Line 11		John Large
	7		Lines 16-21, 30-39		Mike O'Neil
	8		Lines 17-18, 27-29, 33-36, 44-45		Mike O'Neil
	9		Lines 36-39		Mike O'Neil
	10		Lines 1-6		Mike O'Neil
Staff's Official Workpaper (FPL)	146	Y	Lines 5-6	(c)	John Large
	147		Line 12		John Large
	148		Lines 13-16		Mike O'Neil
	153		Lines 31-32		John Large
	162		Line 34		John Large
	172		Lines 14-21		Mike O'Neil
	173		Lines 4-19		Mike O'Neil
	185		Lines 7-25		John Large
	186		Line 18		John Large
	187		Lines 11		Mike O'Neil
	187		Lines 24-29, 38-43		John Large
	188		Lines 26, 31-34, 44-47, 54		John Large
	189		Lines 1-4		John Large

Description	Page Number	Conf. Y/N	Line/Column	366.093(3) F.S.	Affiant
Staff's Official Workpapers (FPL) cont.	192 194 195 199		Lines 24, 26 Lines 36-43 Line 17 Lines 37-41	(c)	John Large John Large John Large Mike O'Neil

EXHIBIT D

AFFIDAVIT

EXHIBIT D
BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

Review of Physical Security Protection of Utility Substations and Control Centers

STATE OF FLORIDA)
) **AFFIDAVIT OF MICHAEL C. O'NEIL**
COUNTY OF PALM BEACH)

BEFORE ME, the undersigned authority, personally appeared Michael C. O'Neil who, being first duly sworn, deposes and says:

1. My name is Michael C. O'Neil. I am currently employed by Florida Power & Light Company as Director, Power Delivery Compliance and Regulatory. My business address is 15430 Endeavor Dr. , Jupiter, Florida, 33478. I have personal knowledge of the matters stated in this affidavit.

2. I have reviewed Exhibit C and the documents that are included in Florida Power & Light Company's ("FPL") Request for Confidential Classification concerning information provided in response to the Review of Physical Security Protection of Utility Substations and Control Centers for which I am identified on Exhibit C as the affiant. The documents and materials that I have reviewed contain proprietary confidential business information, including information relating to security measures, systems, or procedures. The disclosure of this proprietary confidential business information would jeopardize the safe operation of FPL's electrical system. To the best of my knowledge, FPL has maintained the confidentiality of these documents and materials.

3. Consistent with the provisions of the Florida Administrative Code, such materials should remain confidential for a period of not less than eighteen (18) months. In addition, they should be returned to FPL as soon as the information is no longer necessary for the Commission to conduct its business so that FPL can continue to maintain the confidentiality of these documents.

4. Affiant says nothing further.

Michael C. O'Neil

SWORN TO AND SUBSCRIBED before me this 24th day of November 2014, by Michael C. O'Neil who is personally known to me or who has produced personally known (type of identification) as identification and who did take an oath.

My Commission Expires:

Traci D. Goldwire
Notary Public, State of Florida

TRACI D. GOLDWIRE
Notary Public - State of Florida
My Comm. Expires Jul 31, 2015
Commission # EE 117539

EXHIBIT D
BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

Review of Physical Security Protection of Utility Substations and Control Centers

STATE OF FLORIDA)
) **AFFIDAVIT OF JOHN LARGE**
COUNTY OF PALM BEACH)

BEFORE ME, the undersigned authority, personally appeared John Large who, being first duly sworn, deposes and says:

1. My name is John Large. I am currently employed by Florida Power & Light Company as Sr. Manager of Corporate Security. My business address is 700 Universe Blvd., Juno Beach, Florida, 33408. I have personal knowledge of the matters stated in this affidavit.

2. I have reviewed Exhibit C and the documents that are included in Florida Power & Light Company's ("FPL") Request for Confidential Classification concerning information provided in response to the Review of Physical Security Protection of Utility Substations and Control Centers for which I am identified on Exhibit C as the affiant. The documents and materials that I have reviewed contain proprietary confidential business information, including information relating to security measures, systems, or procedures. The disclosure of this proprietary confidential business information would jeopardize the safe operation of FPL's electrical system. To the best of my knowledge, FPL has maintained the confidentiality of these documents and materials.

3. Consistent with the provisions of the Florida Administrative Code, such materials should remain confidential for a period of not less than eighteen (18) months. In addition, they should be returned to FPL as soon as the information is no longer necessary for the Commission to conduct its business so that FPL can continue to maintain the confidentiality of these documents.

4. Affiant says nothing further.

John R. Large
John Large

SWORN TO AND SUBSCRIBED before me this 24th day of November 2014, by John Large who is personally known to me or who has produced personally known (type of identification) as identification and who did take an oath.

My Commission Expires:

Traci D. Goldwire
Notary Public, State of Florida

TRACI D. GOLDWIRE
Notary Public - State of Florida
My Comm. Expires Jul 31, 2015
Commission # EE 117539