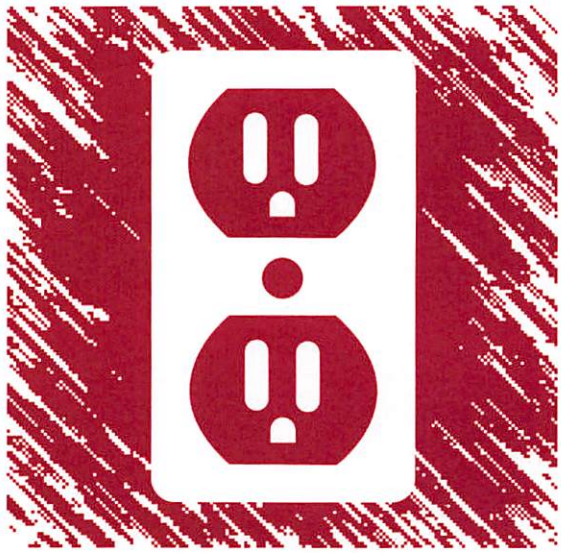


Review of
Physical Security Protection of Utility Substations and Control Centers

December 2014

by authority of

The Florida Public Service Commission
Office of Auditing and Performance Analysis

Review of Physical Security Protection Of Utility Substations And Control Centers

Carl Vinson
Public Utilities Supervisor
Project Manager

Jerry Hallenstein
Senior Analyst

William "Tripp" Coston
Public Utility Analyst IV

R. Lynn Fisher
Government Analyst II

Sofia Delgado Perusquia
Public Utility Analyst II

December 2014

By Authority of
The State of Florida
Public Service Commission
Office of Auditing and Performance Analysis

PA-14-05-003

TABLE OF CONTENTS

7.0 APPENDICES

TABLE OF EXHIBITS

1.0 Executive Summary

1.1 Purpose and Objectives

In May 2014, the Florida Public Service Commission's (FPSC or Commission) Office of Auditing and Performance Analysis initiated a review of physical security measures protecting transmission and distribution substations and system control centers at the four major investor-owned electric utilities in Florida. The purpose of the audit was to develop an understanding of each utility's approach to providing physical security for its substations and associated control centers. The companies included were:

- Duke Energy Florida, Inc. (DEF)
- Florida Power & Light Company (FPL)
- Gulf Power Company (Gulf)
- Tampa Electric Company (TEC)

Audit staff also examined each company's approach to analyzing, improving, and measuring physical security. The primary objectives of the audit were to:

- Review and assess policy documents, plans, and procedures governing physical security of substations and system control centers.
- Identify the internal organization(s) responsible for physical security oversight of company operations.
- Document risk and vulnerability assessments used to select present physical security controls and to identify critical assets.
- Determine methods of compliance with the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) reliability standards approved by the Federal Energy Regulatory Commission (FERC)
- Identify lessons learned and actions taken as a result of 2013 Pacific Gas and Electric Company (PG&E) Metcalf substation attack.
- Document internal company drills, exercises, or external industry simulations used to identify needed improvements and verify readiness.
- Determine extent and impact of additional physical security costs.
- Document information sharing with national and state regulatory agencies and between utilities.
- Document roles and interactions with federal, state and local law enforcement.
- Assess overall impact of the new NERC CIP-014 reliability standard regarding physical security protection.

1.2 Scope

Given these objectives, the scope of the audit focused on the companies' overall approaches and methods for administering and implementing substation and system control center physical security. Audit staff focused upon both the security measures currently in place and ongoing utility efforts to assess the potential threats and vulnerabilities of these facilities to a physical attack.

Audit staff reviewed each company's current compliance efforts related to NERC's Critical Infrastructure Protection reliability standards, and examined each company's plans to comply with new or changing CIP requirements.

1.3 Methodology

Planning, research, and data collection for this audit were performed during May 2014 through October 2014. The information compiled in this audit report was gathered through responses to document requests and onsite interviews with key employees accountable for directing, developing, and implementing each utility's physical security plans and procedures. Specific information collected and reviewed from each utility included:

- Physical security program policies and procedures;
- Substation and control center risk assessments and inspections;
- Costs for physical security;
- Recovery and response policies and procedures;
- Occurrences of physical security incidents; and
- Actions taken in response to PG&E Metcalf substation attack.

1.4 Audit Staff Observations

Federal regulations such as NERC CIP requirements, and actions by the Department of Homeland Security, Department of Energy, and other agencies have laid a solid foundation for protecting the most critical Bulk Electric System sector assets operated by Florida IOUs.

Federal policy efforts began in the 1990s to protect against cyber and physical attacks and accelerated greatly after the World Trade Center attack on September 11, 2001. The required protections continue to be examined and strengthened. Florida IOUs appear to be appropriately complying with and responding to these requirements.

Audit staff believes the Commission should actively monitor these federal requirements and interact with the agencies involved through various existing information-sharing channels. This monitoring and participating will allow the Commission to ensure that all Florida system assets are appropriately protected, and to keep abreast of actions being taken by Florida IOUs.

Extensive efforts and unknown levels of costs lie ahead for Florida IOUs to comply with NERC reliability standards CIP-002 through CIP-014.

Implementation of Version 5 of existing CIPs will continue through 2017. Though FERC's final order has not yet been issued, the implementation by Florida IOUs of CIP-014 requirements will continue through 2017 and beyond as needed to comply with CIP-014. Each Florida IOU examined in this review is executing a comprehensive plan to accomplish Version 5 implementation and is preparing for CIP-014 implementation pending final resolution of its requirements.

The April 2013 PG&E Metcalf substation physical attack was the most ambitious in the U.S. to date, but questions remain about its implications for protections needed by Florida IOUs.

The appropriate and warranted level of response to the Metcalf substation attack by utilities remains unclear. Though costly to PG&E, the attack failed to disrupt the Bulk Electric System and *no customers lost service*. It is audit staff's understanding that the event fails to qualify under FBI criteria as an act of intentional terrorism. Other potential motivations include retribution by disgruntled former employees.

Florida IOUs have appropriately studied the event and have either implemented or are evaluating changes and new measures. Audit staff believes the Commission should continue to monitor the results of these decisions and efforts.

Selecting and implementing prudent, proportionate preparations against physical attack necessarily entails value judgments. Continuous vigilance and frequent reassessment of risk analysis and threat analysis should be employed by Florida IOUs.

To date, very few physical attack events targeting the U.S. transmission grid have occurred, resulting in negligible damage and disruption. However, future attacks could have some success in disrupting the Bulk Electric System grid. Unfortunately, future actual attacks and prevented plots will be one of the best indicators to guide regulators and utilities towards the optimal levels of protection and expenditures.

In recent years and months, Florida IOUs have reassessed their structural and procedural approaches to physical security protection. In many cases, new work units and procedures are under development. The extent of formalization of risk analysis activities varies, as do facilities inspection activities and deployment of security equipment. Audit staff believes increased active information sharing among Florida IOUs may provide worthwhile benefits.

All assets of Florida IOUs within the Florida Public Service Commission's jurisdiction (i.e., below 100kV) fall outside of existing NERC CIP reliability standards.

Distribution substations and smaller transmission substations are likely viewed by most attackers intent on system disruption as low-priority targets. Loss of these substations could have limited impact in comparison to other potential transmission targets, and most outages could be mitigated with minor customer impact through rerouting power.

With existing NERC CIP requirements focusing on the most critical potential targets, protection of the remaining assets remains under the discretion of the IOUs. NESC safety requirements and company practices have provided a reasonable level security for substations in the past.

Audit staff's analysis shows relatively few intrusion and damage incidents at Florida IOUs substations over the period 2011 through mid-2014. Rather than system disruption, the prevalent motive has been copper theft, and an overall declining trend for that category is observable. Though conceivable and worthy of preventative preparations, audit staff believes that an attack on a Florida distribution or small transmission substation intended to cause total substation shutdown represents a low-probability, low-impact event.

The Florida Public Service Commission and Florida IOUs should work cooperatively to identify the appropriate, prudent and cost-effective levels of protection needed.

Audit staff believes the Commission's role in participating with Florida IOUs in the review of the adequacy of protections and preparations should be examined and clarified. Some Commission rules currently address safety and operational activities related to system protection, reliability, and resiliency.

However, the Commission may need to consider the need for periodic reporting of specific information related to Florida IOUs' efforts to detect, prevent, and recover from physical attack against their key system assets. Workshops or docketed proceedings could be used to initiate information exchange, and provide a basis for analysis of the Commission's needs and appropriate role in monitoring protection against physical attack.

Prudent investment by Florida IOUs related to physical security should be based upon focused risk assessments. Since costs must be weighed against potential benefits and perceived risks, cost recovery of physical security costs may become a significant issue.

Investment and expenses related to physical security will rise in the future. System "gold plating" could provide a high degree of protection with a high cost burden on ratepayers. Audit staff believes Florida IOUs would benefit from guidance from the Florida Public Service Commission as they face investment decisions.

To effectively deal with cost recovery, additional efforts by utilities to identify and separately account for these costs may be necessary. Audit staff also believes the Commission will benefit from focused discussion of these expenditures in company filings and testimony.

2.0 Background and Perspective

2.1 Federal Critical Infrastructure Protection Initiatives

Critical infrastructure protection (CIP) includes wide-ranging efforts to fortify, protect, and, if need be, quickly repair or replace vital systems and services. Not only is physical infrastructure itself vulnerable to conventional methods of destruction such as explosives, but computers and networks that control them are at risk from malware and viruses. Utilities depend heavily on information technology to control many basic transmission and distribution functions.

In July 1996, via an Executive Order, the President's Commission on Critical Infrastructure Protection (PCCIP) charter was created. The purpose of the charter was to report the scope and nature of the vulnerabilities and threats focusing primarily on cyber threats.

In May 1998, as a follow-up to the PCCIP's report, a Presidential Directive (PDD-63) was issued to mandate the formation of a national program of critical infrastructure protection. The Directive called on the Federal government to improve cooperation and information sharing between Federal agencies and the private sector to ensure the continuity and viability of critical physical and cyber-based infrastructures, with primary focus on cyber security. The Directive identified major sectors of the nation's critical infrastructure that need to be protected (e.g., energy, banking, transportation, emergency services), and appointed a lead federal agency to interact with each of these sectors. The Department of Energy (DOE) was appointed as the lead agency for the energy sector.

One of the most significant initiatives that stemmed from the heightened focus on infrastructure protection was the creation of Information Sharing and Analysis Centers (ISACs) in 2000. ISACs were formed to promote collaboration and information sharing both between government and industry and within key industries with respect to threats. ISACs primarily serve as means of partnering for the protection of critical infrastructure. The North American Electric Reliability Corporation (NERC) is responsible for operating the ISACs for the energy sector.

In the wake of the September 11, 2001 terrorist attacks, the President signed two Executive Orders relevant to critical infrastructure protection. One established the Department of Homeland Security and the second established the National Infrastructure Advisory Council (NIAC). The Council's functions include enhancing public-private partnerships, monitoring the development of ISAC, and encouraging the private sector to perform periodic vulnerability assessments of critical information and telecommunication systems.

The policies and roles of the various agencies regarding critical infrastructure protection, as outlined in previous Directives and Executive Orders, were codified in a 2003 Presidential Directive (HSPD-7). This 2003 Directive established a deadline for all federal agencies to develop critical infrastructure protection plans and submit those plans for approval by July 2004. By June 2006, an integrated National Infrastructure Protection Plan (NIPP) was in place. The latest version of the Plan was produced in 2013. In general, the NIPP defines and standardizes, across all the major sectors, the process for determining risk and identifying potential risk mitigation activities. The NIPP is considered to be a mechanism for developing coordination between government and the private sector.

2.2 Recent Physical Security Incidents

2.2.1 PG&E Metcalf Substation Attack

On April 16, 2013, the Pacific Gas and Electric Company (PG&E) Metcalf transmission substation near San Jose, California sustained a highly organized attack. Intruders cut the underground telecommunication fiber optic cables but did not fully disrupt the telemetry between the PG&E substation and the control center. The attackers shot the large transformer bank, firing 100 to 150 rounds of rifle ammunition. Of the 20 transformers, 17 were damaged as oil leaked and caused them to overheat. This triggered an alarm signaling the control center that the equipment was in distress, and the transformers were safely switched off to prevent further damage. The control center operators dispatched technicians and contacted security personnel.

Law enforcement responding did not have a fundamental understanding of the substation layout and equipment to assess the situation. The PG&E control center was able to reroute power to avert any costumer outages in the San Jose area. The FBI was notified, and guards were posted outside the substation to deter any subsequent attack. To date, no suspects have been apprehended.

Despite the fact that no outage to customers occurred, this has been seen as a landmark event in electric grid security. The electric industry as a sector responded quickly to the event. This attack eventually attracted a significant amount of public interest in early 2014 and heightened public awareness of the challenges facing the security of the electric grid. The Metcalf incident highlighted the vulnerabilities of the electric industry and triggered utilities in Florida and across the country to perform self-assessments to determine the adequacy of their security. It also prompted federal agencies and sector groups to begin thinking of improvements to the industry's general approach to physical security. Many utilities across the country used the Metcalf attack as a case study to enhance their own security measures. Some of the needs identified by the PG&E Metcalf incident include:

- Better law enforcement communication and education of substations;
- Training on substation equipment for corporate security personnel;
- Further hardening of facilities critical to the reliability of the grid; and
- Improvements in the response time to incidents.

2.2.2 Other Physical Security Events

Aside from the Metcalf attack, there have been few notable physical security incidents around the country in recent years. A transmission line and tower were compromised in central Arkansas on August 21, 2013. By attaching a cable to the framework of a transmission tower and across a railroad track, perpetrators intended to use a passing train to bring down a transmission line. This attempt failed, and no suspects have been identified. Also in Arkansas, on September 29, 2013, a substation control house was set on fire. There were no injuries or customer outages. A suspect was apprehended and found responsible for the arson. **Appendix 1** shows additional physical security intrusion and sabotage incidents that occurred at electric substations nationwide from 2010 to date. Incidents motivated by theft of copper have been excluded since they largely do not involve an attempt to disrupt system operations.

2.3 NERC CIP Physical Security Reliability Standard

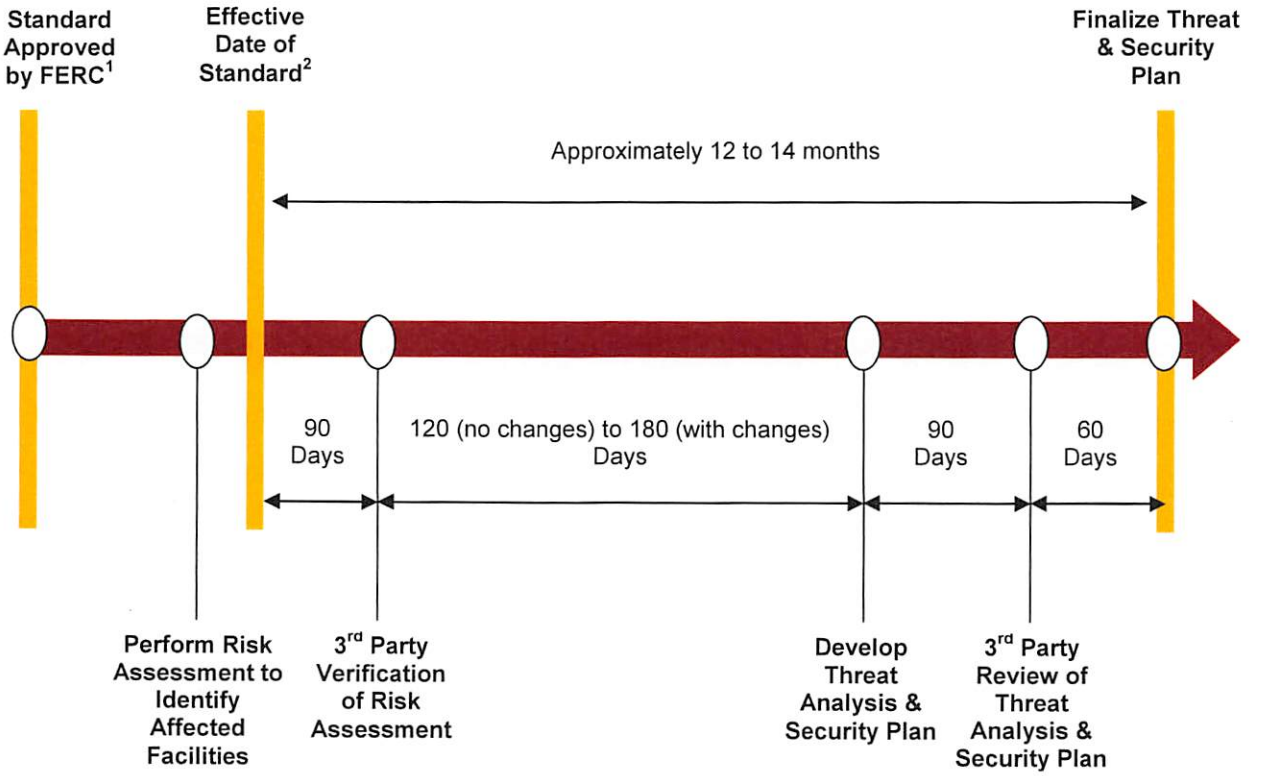
On August 14, 2003, a widespread blackout occurred throughout the Northeastern and Midwestern United States and parts of Canada. The blackout resulted from overloaded transmission lines that hit unpruned foliage and the failure of an alarm to notify operators of the need to re-distribute power. In response, the Energy Policy Act of 2005 set federal reliability standards to regulate the electric grid. With oversight by the Federal Energy Regulatory Commission (FERC), NERC was designated as the entity responsible for developing the standards.

Over 100 reliability standards exist that regulate areas such as communications and coordination, emergency preparedness operations, interconnection reliability operations and coordination, demand reporting, nuclear plant interface coordination, operating personnel responsibility, and critical infrastructure protection. Failure to comply with the requirements may trigger sizable penalties of as much as one million dollars per day per violation. As will be discussed in detail in section 2.5, eight of the reliability standards approved by FERC in 2008 relate to *cyber security of critical infrastructure*.

In response to the PG&E Metcalf attack in 2013, FERC moved quickly to address the highlighted weaknesses in the *physical security of the electric grid*. By June 2014, NERC had drafted, approved and filed with FERC its proposed reliability standard regarding physical security. The primary objective of the proposed reliability standard, CIP-014, as stated in the purpose statement is: "To identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or cascading within an interconnection." Unlike other NERC CIP standards, CIP-014 focuses on the physical security of the entire substation facility as opposed to the *cyber asset*; it is the first NERC *physical security* standard addressing critical infrastructure protection imposed on the electric sector.

Exhibit 1 shows a proposed timeline of the implementation of CIP-014. The reliability standard was recently approved by FERC on November 20, 2014. The next step is for each utility to perform a risk assessment to identify critical substations and control centers which could cause a widespread cascading effect or instability to the grid due to the loss of the facility. CIP-014 further requires third party verification of the risk assessment used by the utilities to identify facilities. This third party verifier must be unaffiliated with the utility and have transmission planning or analysis experience. Once a third party verifies a utility's risk assessments, a threat and vulnerability evaluation is conducted and a security plan is developed for each identified critical facility by the utility. A third party review of the threat and vulnerability evaluation and security plan must then be conducted. After this review is completed, the utility can begin implementation of physical security plans. The entire process of developing and reviewing a security plan is estimated to take 12 to 14 months after the effective date of the standard. Based on the current status of CIP-014, the projected effective date for the standard is summer of 2015.

CIP-014 Timeline



[1]Approved on November 20, 2014
[2]Anticipated Summer 2015

EXHIBIT 1

Source: Edison Electric Institute

2.4 Physical Security Industry Guidelines

2.4.1 NERC Security Guideline

In recent years, NERC established a series of voluntary guidelines for the electric industries' approach and response to physical security of assets. Specifically, NERC developed guidance documents for use in the area of overall physical security approach and in the area of responding to national security threats.

NERC Security Guidelines Electricity Sector: Physical Security

In June 2001, NERC approved "An Approach to Action for the Electric Sector." This guidance establishes a four-tiered approach to physical security of utilities' assets. Specifically this document identifies the areas of:

- Avoidance
- Assurance
- Detection
- Recovery

For each of these areas, the utility is charged with developing an approach to deter or protect its assets from physical attack. Within this four-tier approach, the guideline establishes a series of concepts to implement a response and mitigate the impact of an attack. The guidelines provide specific detail on how a utility should approach the physical protection of its assets from attack.

In June 2012, NERC developed a set of guidelines for physical security for the electric system, titled *NERC Security Guidelines Electricity Sector: Physical Security*. Furthermore, the guidelines recommend that each utility have in place a physical security process to safeguard both its employees and essential physical assets. The companies are also encouraged to use risk-based assessments to identify and evaluate the critical components.

NERC Security Guideline for the Electricity Sub-sector: Physical Security Response

In October 2013, NERC revised and reissued the *NERC Security Guideline for the Electricity Sub-sector: Physical Security Response*. This document provides guidelines for its physical security approach specifically for responding to various national security threat levels. This guideline focuses on approaches to mitigating the risks associated with the potential, and actual, threat of a physical security attack and how to respond to such events. However, NERC reiterates that this guideline is not intended to be a complete and all-inclusive approach, but a base-line guidance approach to threat response. The goal of these guidelines is to support utilities' development of response to threat alerts and provide examples of appropriate responses on how a threat should be addressed by a utility.

The guideline delineates three threat levels: *Normal, Elevated*, and *Imminent Risk*. The expectation is that all utilities should incorporate these guidelines within its overall threat-response procedures. The *Normal* level provides guidance on how the company should approach its physical security under its routine, day-to-day approach. An *Elevated* risk occurs when a credible threat of terrorism or criminal activity against the utility industry is identified. Finally, the *Imminent* level is when an actual terrorist event or criminal act against the utility industry occurred, or when a highly credible threat is present **Appendix 2** provides a full listing of suggested activities and responses to the three national threat levels.

2.4.2 Additional Regulatory and Industry Support

In addition to the NERC guidance documents, there are a number of other governmental and industry organizations that provide physical secure guidance, and assistance to utilities. The National Electrical Safety Code (NESC) establishes general requirements for protecting electric supply stations. These standards are found in the NESC, Section 11, and provide specific guidance for securing both the substation physical perimeter and the equipment located within the site. Specific guidance includes fencing/perimeter barriers, clearance and height parameters, signage, and lightning. The four companies evaluated within this report use this standard as its baseline for securing their substations.

The Department of Homeland Security has numerous committees in place that provide oversight and guidelines to utilities on how to secure and protect critical assets. One specific committee, the National Infrastructure Advisory Council, provides critical insight to utilities and other industry sectors on protecting the country's critical infrastructure.

There are additional federal and industry advisory groups that provide support in the areas of physical and cyber security. These groups provides assistance to utilities as a resources and conduit for sharing industry-related security issues. Examples include, but are

not limited to, the FBI Domestic Security Advisory Committee, Department of Homeland Security Protective Security Advisors, the Secret Service, the Regional Domestic Security Task Force, Florida Fusion Centers, the North American Transmission Forum, and the Edison Electric Institute.

2.5 NERC CIP Cyber Security Reliability Standards

As noted, the original set of NERC CIP reliability standards approved by FERC in 2008 all related primarily to critical infrastructure protection of *cyber assets*. Within these NERC CIP reliability standards (CIP-002 through CIP-009) there are 176 requirements that address the cyber and physical protection of critical facilities and their associated *"cyber assets"*. Cyber assets are any programmable electronic devices and communication networks including hardware, software and data. Currently, only the Bulk Electric System is subject to mandatory standards for cyber security. **Exhibit 2** displays CIP-002 through CIP-009 and a brief description of each.

NERC
Critical Infrastructure Protection Reliability Standards
Version 3

NERC Standard	Requirement
CIP-002	Requires the identification of critical assets and their associated critical cyber assets that support the reliable operation of the Bulk Electric System.
CIP-003	Requires security management controls in place to protect critical cyber assets
CIP-004	Requires that personnel have an appropriate level of personnel risk assessment, training.
CIP-005	Requires protection of the electronic security perimeters inside which all critical cyber assets reside, as well as all access points on the perimeter.
CIP-006	Addresses implementation of a physical security program for the protection of critical cyber assets.
CIP-007	Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets.
CIP-008	Ensures reporting of cybersecurity incidents related to critical cyber assets to the ISAC.
CIP-009	Ensures that recovery plans are in place for critical cyber assets

EXHIBIT 2 *Source: NERC Reliability Standards*

Under these NERC CIP standards, utilities are required to identify critical cyber assets and to regularly perform a risk analysis of those assets. Additionally, NERC CIP requires the use of firewalls and other cyber security measures to block against cyber attacks and to create comprehensive contingency plans for cyber attacks, natural disasters and other unplanned events. Policies and procedures must be developed for monitoring and changing the configuration of critical assets and governing access to those assets.

Electric utilities currently are governed by Version 3 of the NERC CIP standards approved by FERC in 2010. However, by April 2016, utilities must also transition to implement

Version 5[1] of the NERC CIP standards that were approved by FERC in November 2013. Hence, the utilities must maintain a compliant status under Version 3 while working to implement the additional requirements of Version 5.

NERC CIP Version 5 significantly revises the scope of the NERC CIP Standards and the protections applied to identified assets. A major investment of time and resources, will be required by each of the utilities to comply with NERC CIP Version 5 by April 2016. Under the existing NERC CIP Version 3, utilities are required to identify critical assets through their own risk based assessment methodology and only the *critical* cyber assets associated with those assets are covered by the requirements in the standards. Under NERC CIP Version 5, utilities are required to identify their critical assets through application of a bright-line criteria. For the first time, *all* cyber systems associated with those critical assets that, if compromised, may impact the Bulk Electric System will be subject to some form of protection and will now fall within the scope of compliance with NERC standards.

2.6 NERC CIP Compliance

Under NERC's authority, the following eight regional entities are responsible for monitoring and enforcing compliance with the approved NERC reliability standards.

- Florida Reliability Coordinating Council, Inc. (FRCC)
- Midwest Reliability Organization
- Northeast Power Coordinating Council
- Reliability First Corporation
- SERC Reliability Corporation (SERC)
- Southwest Power Pool
- Texas Regional Entity
- Western Electricity Coordinating Council

Gulf Power Company falls under the jurisdiction of the SERC Reliability Corporation (SERC) while Florida Power & Light Company, Duke Energy Florida, and Tampa Electric Company fall under the responsibility of the Florida Reliability Coordinating Council, Inc. (FRCC). Both the FRCC and SERC conduct NERC CIP compliance audits on a prescribed schedule ensuring that each utility is subject to an audit every three years. Audit staff has verified that these audits have been conducted as required for each utility in this review.

2.7 Florida Public Service Commission Jurisdiction

2.7.1 Florida Statutes

Chapter 366 of the Florida Statutes (F.S.) grants various powers to the Florida Public Service Commission related to the physical security of Florida utilities infrastructure. Section 366.04(5), F.S., provides the Commission with "jurisdiction over the planning, development, and maintenance of a coordinated electric power grid throughout Florida." Under the statute, the Commission is also tasked to "assure an adequate and reliable source of energy for operational

[1] CIP Version 4 reliability standards did not go into effect as scheduled. Instead, utilities will transition directly from the Version 3 Standards to the Version 5 Standards.

and emergency purposes in Florida", and to avoid "uneconomic duplication of generation, transmission, and distribution facilities".

Section 366.04(6), F.S., gives the Commission "exclusive jurisdiction to prescribe and enforce safety standards for transmission and distribution facilities of all public electric utilities, cooperatives organized under the Rural Electric Cooperative Law, and electric utilities owned and operated by municipalities."

Under Section 366.05(1), F.S., the Commission is given powers to "prescribe fair and reasonable rates and charges, classifications, standards of quality and measurements, including the ability to adopt construction standards that exceed the National Electrical Safety Code." Additionally, the Commission is empowered to require the "repairs, improvements, additions, replacements, and extensions to the plant and equipment of any public utility when reasonably necessary."

Section 366.05(8), F.S., states that if the "commission determines that there is probable cause to believe that inadequacies exist with respect to the energy grids developed by the electric utility industry" then the Commission has the power to require installation or repair of necessary facilities, including generating plants and transmission facilities.

2.7.2 FPSC Rules

FPSC Rule 25-6, Florida Administrative Code (F.A.C.), titled *Electric Service By Electric Public Utilities*, is designed to define and promote good utility practices and procedures, to ensure adequate and efficient service at reasonable costs, and to establish the rights and responsibilities of the utility and the customer.

Florida's transmission system consists of lines rated at 69 kV, 115 kV, 138 kV, 230 kV, and 500 kV. While the NERC Critical Infrastructure Protection reliability standards exist to protect the Bulk Electric System, similar physical and cyber standards are not afforded to the distribution grid. The Commission has jurisdiction of transmission lines less than 100 kV and the distribution electrical system throughout Florida. The distribution system comprises all lines at voltages lower than 69 kV.

Exhibit 3 lists several existing Commission Rules that speak to:

- Construction of new transmission and distribution facilities
- Recording interruptions and threats to the Bulk Electric System
- Capacity shortage emergencies
- Notification of electric utility outage events, and
- Inspection of utility plant

FPSC Rules for Transmission and Distribution Facilities	
Rule	**Purpose/Description**
25-6.018	***Records of Interruptions and Commission Notification of Threats to Bulk Power Supply Integrity or Major Interruption of Service,*** ... notification of certain situations, including any bulk power supply malfunction or accident which constitutes an unusual threat to the bulk power supply integrity.
25-6.0183	***Electric Utility Procedures for Generating Capacity Shortage Emergencies***, adopts the Florida Reliability Coordinating Council's Generating Capacity Shortage Plan ... to address generating shortage emergencies within Florida.
25-6.0185	***Electric Utility Procedures for Long-Term Energy Emergencies***, ... requires a long-term energy emergency plan to establish a systematic and effective means of anticipating, assessing, and responding to a long-term emergency caused by a fuel supply shortage.
25-6.019	***Notification of Events***, ... must report to the Commission within 30 days of learning about any event involving a portion of the electrical system involving damage to the property of others in excess of $10,000, or causing significant damage in the judgment of the utility to its facilities.
25-6.0343	***Municipal Electric Utility and Rural Electric Cooperative Reporting Requirements***, ... reports include a description of each municipal and electric cooperative's planned facility inspections for transmission and distribution facilities including the number and percentage of transmission and distribution inspections planned and completed annually and the utility's quantity, level, and scope of vegetation management planned and completed for transmission and distribution facilities.
25-6.0345	***Safety Standards for Construction of New Transmission and Distribution Facilities***,.. adopts and incorporates the 2012 edition of the National Electric Safety Code (ANSI C-2) as the applicable safety standards for transmission and distribution facilities subject to the Commission's safety jurisdiction..
25-6.036	***Inspection of Plant*** ... requires each electric utility to adopt a program of inspection for its electric plant to determine the necessity for replacement and repair.

EXHIBIT 3 *Source: Rule 25-6, F.A.C.*

3.0 Duke Energy Florida, Inc.

3.1 Security Management

3.1.1 Security Organization

Duke Energy's corporate Enterprise Protective Services organization is responsible for the physical security operations for each of its regions, including Duke Energy Florida (DEF). Enterprise Protective Services' responsibilities include:

- Physical and Technical Security
- Corporate Investigations
- Pre-employment Screening
- Enterprise Business Continuity
- Enterprise Crisis Management
- Non-regulated Drug and Alcohol Testing
- Security Regulatory compliance
- Executive Protection
- Local, State and Federal Law Enforcement Liaison

The Enterprise Protective Services organization is headed by a Managing Director who reports directly to the Vice President of Administrative Services for Duke Energy Corporation. The Managing director is responsible for oversight of the following four business units, each headed by a director:

- Operational Security Investigations
- Security Risk and Compliance
- Infrastructure Protection
- Preparedness Services and Business Continuity

In response to the PG&E Metcalf transmission substation attack, Duke Energy senior management determined that resources should be specifically dedicated to physical security protection. In 2014, a new business unit, Physical Security Projects, was created within the Enterprise Protective Services organization to oversee transmission physical security protection and the development and implementation of NERC's CIP-014 reliability standard.

Duke Energy Corporation also uses an Enterprise Security Command Center to provide centralized monitoring of critical sites such as generation facilities, control centers, substations, and office buildings. The Command Center operates 24 hours every day, and through the use of virtual and visual information can automatically analyze and correlate alerts across DEF's service territory. Alerts that come into the Command Center are overlaid on a map-based interface to allow operators to quickly pinpoint and direct response personnel to the alert's exact location. For facilities that require heightened security on an as-needed basis, Enterprise Protective Services may deploy mobile security cameras to monitor activity. Mobile surveillance is monitored by a third-party contractor and the Command Center oversees the contractor's operations.

3.1.2 Physical Security Policies and Plans

Duke Energy Corporation employs a multi-tiered approach to grid security that is based on resiliency and includes elements of prevention and response to system threats. The approach includes:

- Internal working teams specifically focused on physical security and threats
- Functionally managed regional security groups
- Participation in industry groups
- Coordination of information sharing
- Development of emergency response and business continuity plans
- Participation in annual emergency drills
- Participation in spare equipment plans and programs (EEI STEP)

The physical security policy and general responsibilities for DEF are defined in its corporate *Physical Security Program* procedures. The procedures describe the processes for conducting physical security evaluations and recommends minimum security features for all transmission and distribution facilities. The procedures further establish categories for facilities, such as office complexes, generation facilities, and substations. Within each facility category are various levels of security and associated minimum security requirements based on facility criticality. For example, a transmission substation that is determined to be critical to Duke's business operations would fall into a higher level of security than a distribution substation and would be equipped with additional security equipment.

As part of physical security protection, Duke Energy Corporation is also required to have a physical security plan for the protection of *cyber assets.* NERC CIP-006 specifically requires Duke Energy Corporation to have an effective physical security plan to ensure proper access controls are in place to protect critical *cyber assets.* At a minimum, the physical security plan must address perimeter protection of cyber assets, physical access points, protection of control systems, protection of electronic access control systems, and procedural controls for monitoring physical access.

Duke Energy Corporation employs an *Employee Screening Policy* for all employees, third party suppliers, and sub-contractors who are granted access to key facilities, including both transmission and distribution. Screening components may include social security number verification, criminal history check, terrorist watch database search, professional licenses, and consumer credit background review. NERC standards specifically require identity verification, seven-year criminal check and training for those with unescorted access to critical assets.

To ensure all published procedures are reviewed, Duke Energy Corporation established an Enterprise Document Control program that requires all procedures to be reviewed every two years or more often as needed. All procedures are approved by the Director responsible for the program or content.

3.1.3 Interactions with Law Enforcement and Federal Agencies

DEF works closely with local, state, regional, and federal law enforcement and government agencies including local police, sheriff departments, U.S. Coast Guard, Florida Department of Law Enforcement, FBI, FERC and Department of Homeland Security. Since the PG&E Metcalf substation event, DEF has increased its communication effort with key law enforcement personnel to enhance security monitoring and allow for timely response to any future event.

NERC reliability standard EOP-004-2 requires Duke Energy Corporation to have an event reporting operating plan that includes the protocols for reporting specific events to the Florida Reliability Coordinating Council (FRCC), other utilities, and local law enforcement. Specific events include damage or destruction of a facility, physical threats to the Bulk Electric System and control center, and loss or reduction of load. According to Duke Energy Corporation, there have only been two potentially related security incidents that triggered an EOP-004-2 event report since 2010. An unknown unauthorized individual entered a substation and operated certain equipment resulting in a 16 minute outage to approximately 7,700 customers. One week later a similar incident occurred at the same substation resulting in a 4 minute outage to approximately 7,900 customers.]

Duke Energy Corporation regularly participates in groups including the North American Transmission Forum, Edison Electric Institute, Security Executive Council, American Society for Industrial Security, and Department of Homeland Security Protective Security Advisors. Through these associations, Duke Energy corporate employees share ideas with other utilities and learn from each other's experience.

The corporate Enterprise Protective Services personnel have also been trained as active coordinators in local Fusion Centers that were created under the Department of Homeland Security. The fusion centers, located throughout the states Duke Energy Corporation serves, are a central gathering point for local, state, and federal law enforcement and government agencies to partner and share threat-related information.

3.1.4 Physical Security Cost Tracking

The corporate Enterprise Protective Services organization is funded through an operating budget primarily comprised of employee expenses, contracts, and labor and benefits costs. However, much of the security-related investment and assets are funded through transmission and distribution operations.

Physical security features such as cameras, fencing, and card access readers are included in capital projects or imbedded in other expense categories under operations and maintenance budgets. The broad categories of projects included in DEF's transmission and distribution capital budget makes it difficult to compile the total amount either invested or budgeted specifically for physical security activities.

3.2 Transmission Physical Security Protection

A utility's Bulk Electric System is comprised of generation and transmission facilities and their supporting control centers. FERC's current definition of the Bulk Electric System establishes a "bright-line" threshold that includes all generation and transmission facilities operated at or above 100 kV. The Bulk Electric System does not include facilities used in the local distribution of electric energy. The Florida Public Service Commission's jurisdiction is limited to all transmission facilities operating at or below 99 kV.

If the Bulk Electric System is disrupted, the effects may be felt in more than one location. Facilities included in DEF's portion of the Bulk Electric System include 179 transmission substations and the primary and backup transmission control centers. Following the September 11, 2001 terrorist attacks, DEF enhanced the physical security measures at many transmission substations and the transmission and distribution control center to increase protection.

Examples include [redacted].

3.2.1 Risk and Vulnerability Assessments

Critical cyber asset determination and assessments for DEF's transmission substations and system control center facilities are completed annually as part of the risk based assessment methodology required under NERC CIP-002. The latest assessment was completed in March 2014.

DEF currently uses Progress Energy's legacy risk analysis program to identify and prioritize the most serious potential vulnerabilities and security gaps in the Bulk Electric System. To do so, the following risk assessments are performed:

- Identify most critical Bulk Electric System facilities
- Estimate probability of threats occurring
- Estimate impact of a loss of a critical function or asset
- Document qualitative and quantitative measures used to determine impact levels
- Evaluate compliance with Physical Security Program procedures
- Identify controls to prevent or minimize the effects of potential loss

After the assessments are completed, the risk analysis program tiers critical facilities in accordance to their importance to the reliability or operability of the electric grid. For example, tier 1 substations are those assessed to be the most critical to the company and if removed from the system or damaged would cause a serious or widespread outage.

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 "cube" (walls, ceiling, and floor) that houses the cyber asset. In most cases, the six-wall cube is either the control center or the control house building at a substation. These stations are required under CIP standards to employ security measures above DEF's baseline such as card readers, visitor logs, cameras, and video analytics. All critical and non-critical substations adhere to DEF's baseline security measures, which include a chain-linked fence, concrete block control house, lighting, and locks at station gate and control house.

Duke Energy's Enterprise Services Organization is currently in the process of integrating elements of Progress Energy's legacy risk analysis program into a new corporate *Work Place Security Policy*. The new Policy, to be published in November 2014, will standardize the risk assessment process for all of Duke Energy's service territory and will include procedures to comply with NERC's CIP-014 reliability standard regarding physical security.

To assess security protection, Duke Energy Corporation also monitors criminal activities that occur at its substations. **Exhibit 4** depicts 242 security incidents that occurred in DEF's transmission and distribution substations from 2011 through mid-July 2014. The vast majority of incidents (228) were burglary or theft related. Burglary incidents are those where substation perimeter intrusion was detected, whereas theft incidents are non-intrusive. The exhibit further shows the trend in the total number of incidents over time, from a high of 94 in 2011 to 62 in 2013. For 2014, only 11 incidents have been reported as of July 7.

Duke Energy Florida Transmission and Distribution Substation Security Incidents 2011-2014					
Types of Incidents	**2011**	**2012**	**2013**	**2014***	**Total**
Burglary	51	53	27	3	**134**
Theft	41	22	24	7	**94**
Vandalism	2	0	11	1	**14**
Total	**94**	**75**	**62**	**11**	**242**

Through July 7, 2014.

EXHIBIT 4 *Source: Document Request Response 3-1*

3.2.2 Physical Security Inspection Process

When warranted, corporate Enterprise Protective Services performs security inspections on its transmission substations. When determining which substations to inspect, corporate security considers factors such as new construction or the history of security incidents. The security inspections, also known as property security surveys, are thorough evaluations of existing security methods and systems based on minimum security standards as provided in the company's Physical Security Program procedures.

The inspection process includes, but is not limited to, an assessment of the perimeter fencing, substation structures, and electrical equipment. The final inspection reports include a description of the facility inspected, a brief history of security incidents, a security checklist to specify compliance by component (e.g., lighting and fencing), and recommended corrective action. A work order is to be generated for all deficiencies.

3.3 Distribution Physical Security Protection

Distribution substations connect to the transmission system to reduce the transmission voltage, typically to about 30–60 kV, and terminate at a lower voltage below 1 kV at the customer's premise. DEF currently has 224 distribution substations that fall under the Commission's jurisdiction.

Like transmission substations, minimum physical security protection measures at distribution substations include [redacted]. If needed, security may be enhanced with features such as [redacted]. A disabled distribution substation can be rerouted in a fairly quick order with customer impacts avoided or limited. Therefore, distribution substations are not likely targets of attacks for the purpose of system disruption.

3.3.1 Risk and Vulnerability Assessments

Security protections in place at distribution substations are primarily deployed to mitigate against burglary/theft (often copper ground wire) and vandalism. Distribution substations are typically unmanned and thus somewhat more susceptible to unauthorized access. Risk and vulnerability assessments performed on DEF's distribution substations are primarily done in response to perceived potential weaknesses.

While physical security of all DEF's substations is on the company's radar, the company must answer the fundamental question of what are the most important assets to the organization. The primary driver, at this moment, for substation security is the regulatory push for implementation of CIP-014, requiring physical security protection of the most critical substations and control centers.

3.3.2 Physical Security Inspection Process

[redacted]

Distribution substation inspections are performed when requested by facilities management or if the need arises resulting from a security incident at the substation. During inspections, substation personnel are required to record any deficiencies for generation of work orders. Duke Energy senior management notes that the company's maintenance department inspects substation perimeter fencing as part of routine substation maintenance.

3.4 Recovery and Response

DEF's operations are designed for redundancy and resiliency. DEF's transmission and distribution organizations both have documented recovery plans in place for emergencies whether caused by natural phenomena or other causes. Both transmission and distribution plans establish command and control structures to aid in communications and repair efforts. Both transmission and distribution control centers have backup capabilities and procedures in place. Per NERC Standard EOP-008, Duke must also maintain a fully redundant backup control center certified by both NERC and the FRCC.

Transmission and distribution recovery plans were developed for use when either catastrophic damage to facilities has occurred, or when a wide area severe weather warning, such as a hurricane, is issued. Both plans establish a consistent approach and level of responsibility for response by providing the authority and coordination needed to restore electric service and maintain business continuity. The plans are organized to consolidate authority to system level top down organizational structure for major storm responses and are appropriate for use in recovery from non-storm outages.

Duke Energy Corporation also has business continuity plans that describe response actions for loss of access to a critical facility. The plans are currently being updated to include elements provided in NERC's *Security Guideline for the Electricity Sub-Sector: Physical Security Response* (see Appendix 2). The *Security Guideline* provides utilities with actions they should consider when responding to threat alerts issued by the U.S. Department of Homeland Security and when operating during normal conditions. The updated business continuity plans will be included in new corporate *Work Place Security Policy* to be completed in November 2014.

Following the September 11, 2001 terrorist attacks, Duke Energy Corporation began participating in Edison Electric Institute's (EEI) Spare Transformer Equipment Program (STEP). The Program creates a sharing arrangement among electric utilities to make efficient use of existing transmission spare transformers. The lead time for the manufacture of large substation transformers is typically two years and most are manufactured overseas. The Program carries with it a binding obligation to provide transformers if called upon by another STEP participant.

Additionally, DEF 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 DEF to cope with a generating capacity shortage on its system and to mitigate the impact of the emergency.

Exhibit 5 shows the number of substation unplanned outages since 2011 excluding named storms, that resulted in a customer interruption. The primary causes of the outages were breaker equipment failures, human errors, animals, and transformer failures. None of the outages were caused by a malicious physical security breach. Total unplanned outages have decreased to a low of 70 in 2013 as a result of a substantial decrease in transmission unplanned outages (28) during the year. As of September 30, 2014, DEF reported 47 total unplanned outages.

DUKE ENERGY FLORIDA
TRANSMISSION AND DISTRIBUTION SUBSTATION UNPLANNED OUTAGES*
2011-2014

Year	Distribution Substation Outages	Transmission Substation Outages	Total Outages
2011	35	40	74
2012	41	58	99
2013	42	28	70
2014**	26	21	47
Total	**144**	**147**	**290**

*Excludes outages caused by named storms.
**As of September 30 2014.

EXHIBIT 5

Source: Document Request Response 3-2 and 3-3

3.5 CIP-014 PREPARATIONS

In response to the April 2013 PG&E Metcalf substation incident, Enterprise Protective Services personnel visited the Metcalf site to discuss lessons learned and best practices with Pacific Gas and Electric Company. Additionally, Enterprise Protective Services has reviewed lessons learned and recommendations with Entergy after the August 2013 Arkansas substation attacks. Duke Energy Corporation has since taken numerous steps to address varying processes and inconsistencies in the application of physical security features to protect substations from unauthorized entry. Examples of improvements to existing security systems include:

- Upgraded hardware and software
- Reconfigured network communications
- Enhanced features to alarm systems
- Increased monitoring capability
- Developed a security working group

Duke Energy Corporation has been an active participant in the development of the NERC CIP-014 reliability standard. The purpose of CIP-014 is to enhance the physical security measures for the most critical Bulk Electric System facilities in an effort to lessen the overall vulnerability against physical attacks. While CIP-014 is not expected to be fully implemented

until the summer of 2015, the company is currently evaluating different security technologies to be implemented to mitigate risk once the CIP-014 standard is finalized. According to corporate management, the company is approaching CIP-014 in three separate phases; analysis, design, and implementation. The company presently is in the analysis phase which includes site-by-site vulnerability assessments with the focus on threats, preventive measures, event mitigation, and event recovery.

3.6 Self-Assessments and Exercises

Utilities across the country, including DEF, held a two-day grid security exercise in November 2013, known as GridEX II. The previous GridEX, which took place in November 2011, included DEF and participants from 75 industry and government organizations in the United States and Canada. GRIDEX II exercise involved approximately 200 organizations with more than 1,800 participants. Participants represented all NERC regions, federal agencies, reliability coordinators and small and large utilities across North America.

GridEX II, built on lessons learned from GridEX 2011, was a simulated exercise with no operational impact to the Bulk Electric System that challenged participants through a "worst case" scenario. GridEX II dedicated a significant amount of the scenario to physical security response and coordination by stressing the system through a series of prolonged, coordinated physical and cyber attacks. NERC is planning for GridEX III, which will take place in November 2015. DEF plans to participate.

In addition to DEF's participation in GridEX, the company conducts periodic internal physical security drills in coordination with federal, state, or local emergency authorities. Drills range from tabletop exercises to activating command and control structures. DEF also participates in an annual exercise of cyber security incident response as required by NERC CIP-008. The exercise involves cross-functional input from DEF's business units.

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.

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.[2] 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 6** 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]

*Through June 2014

EXHIBIT 6

Source: Document Request Response 4-2

[2] NERC EOP 004-2 standard

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[3] 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 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

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

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 7** 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]					

* Through September 2014

EXHIBIT 7

Source: Document Request Response 4-2

Exhibit 8 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]					

* 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 9 shows the recent numbers of security incidents that occurred in distribution substations. [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]					

* 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 10** 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**

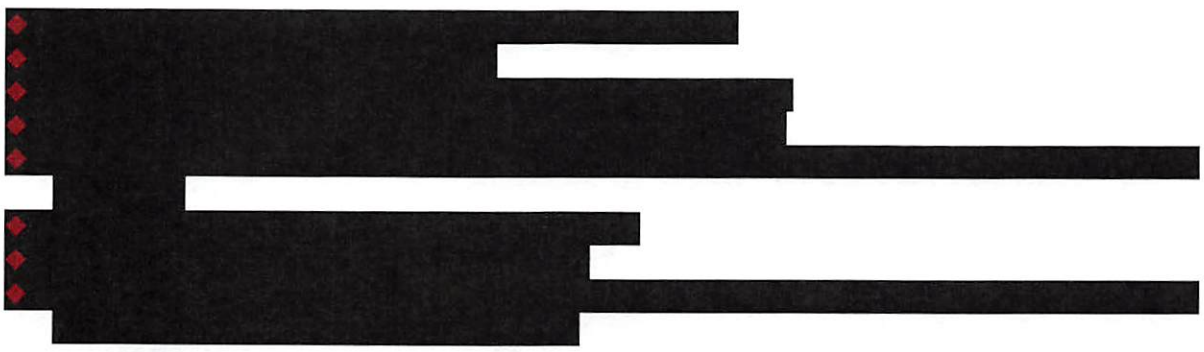
* Excluding outages caused by named storms
** Through August 2014

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:



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-014-1 standard. An FPL Power Delivery employee was a member of the drafting team which developed and wrote the CIP-014 standard. The final version of CIP-014-1 was approved by FERC on November 20, 2014 and becomes effective 60 days after publication in the Federal Register. Consistent with CIP-014-1, FPL has begun to identify the applicable substations. FPL has stated that upon identification of the enhanced security measures at the identified substations and control centers, cost projections will be developed. The new standard encompasses 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.

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.

5.0 Gulf Power Company

5.1 Security Management

5.1.1 Security Organization

As an operating company within Southern Company, Gulf Power Company (Gulf) uses Southern Company's security model in its approach to security management. The Southern Company Security Council is charged with monitoring and overseeing the security of corporate assets. Gulf's Manager of Corporate Security currently serves as the Chairman for the group. The Council also includes security representatives from the other Southern Company utilities. Other committee members contribute expertise in the areas of compliance, business assurance, Information technology, and ethics.

The Security Council ensures the corporation remains aware of potential threats, active attacks, and other security-related issues that could impact the reliability of its infrastructure and safety and of its employees and the public. This group meets monthly to discuss current events within each company and the industry at large. The committee works closely with state and federal agencies as part of its mission.

Gulf's Corporate Security organization is comprised of specialists, many of whom have extensive background in security-related and law-enforcement fields. The company also uses a group of contracted employees who assist Gulf with monitoring its physical assets. Currently, Corporate Security is managed by a Manager Corporate Security, with a team of security investigators. Each investigator is responsible for monitoring and overseeing a specific region of Gulf's service territory.

The primary areas of oversight for Gulf's Corporate Security include:

- Physical/Electronic Security
- Investigations
- Business Assurance
- Access Control
- Uniform Security
- Security Regulations
- Revenue Protection
- Security Training
- Law Enforcement Liaison
- Employee/Executive Protection

The Corporate Security Operation organization operates under a multiple strategy approach for security. The company states that it manages its security using a strategic, risk-based site-specific threat process. This process seeks to effectively predict, detect, deter, delay, and respond to security threats.

Gulf implements this approach by using a number of specialized electronic applications including surveillance cameras, real time card-access readers, alarms, and visitor access controls, which allow the company to monitor strategic locations. The Corporate Security monitors these activities in its centralized monitoring center.

5.1.2 Physical Security Policies and Plans

The Gulf Corporate Security organization has in place a *Gulf Power Corporate Security Business Continuity Plan* and a *Gulf Power Corporate Security Threat Level Response Plan.* These documents address Corporate Security's protocol for managing and responding to a security event or incident. These documents are reviewed annually.

In addition, Gulf's Corporate Security develops a *Security Strategic Plan* that establishes priorities for the organization. These include priorities that focus on physical security, and establish goals for improvement. In 2014, a goal of Corporate Security has been to work with Power Distribution on the issues of equipment and wire thefts.

Gulf has implemented a business contingency directive in its *Gulf Power Business Assurance Policy # 132.* Under this policy, the company is required to have an Incident Response Team, and each business unit—with business critical functionality—is required to develop an Emergency Response Plan and Business Recovery Plan.

Also, per applicable NERC CIP requirements, the company maintains a physical security plan for applicable NERC CIP assets. This document provides details on the specific security standards required under federal rules for each NERC CIP asset. Along with this, the company has a policy for employee and vendor background clearance requirements for those with access to the NERC CIP asset sites.

5.1.3 Interactions with Law Enforcement and Federal Agencies

The company interacts with both state and federal agencies involved in energy sector and national safety issues. Gulf and Southern Company engage with federal agencies such as the Department of Energy, Department of Homeland Security, Regional Domestic Security Task Force, Federal Energy Regulatory Commission, FBI, NERC, and SERC. In several cases, Gulf Power and Southern Company employees are active participants in federal agency and industry group security taskforces.

The company partners with the Florida Department of Law Enforcement and local county law enforcement agencies within its territory to ensure that first-line responders are aware of criticality and safety concerns related to the company's infrastructure. It is the responsibility of each field investigator to maintain and foster the effective law enforcement relations within each geographic region. The company also works with the Florida Fusion Center on threat-related issues within the state.

The company has increased its communication efforts with key partners in light of the PG&E Metcalf substation event. After the 2013 event, Gulf shared needed information regarding substation sites and security monitoring with the appropriate law enforcement groups. The company is developing a Law Enforcement Substation Training and Familiarization program to provide local law enforcement with information and tools to assist in power grid protection.

Gulf and Southern Company interact with NERC in activities related to CIP compliance. NERC EOP-004-2 requires reporting of specific events such as damage or destruction of a facility, threats to the Bulk Electric System, or loss or reduction of load. The utilities must notify specific federal agencies and specific law enforcement groups concerning certain reliability events within its system.

5.1.4 Physical Security Cost Tracking

Much of physical security costs are embedded within the various business units' operating and project budgets. When a new substation is built, or additional resources are added to an existing substation, the cost is included within the capital or O&M budget for the business unit. This makes it difficult for the company to isolate the overall annual physical security cost for these assets.

The Corporate Security organization's budget include salaries, the corporate security monitoring center, and any capital costs associated with security measures implemented specifically by Corporate security. **Exhibit 11** shows the annual Corporate Security budget for 2010 through July 2014 remained stable for the period.

Gulf Power Company
Corporate Security Budget
2010-2014

Year	Capital Expenditures	Operation and Maintenance	Total
2010	$ 40,705	$1,570,045	**$1,610,750**
2011	$ 40,500	$1,620,883	**$1,661,383**
2012	$ 40,500	$1,582,423	**$1,622,923**
2013	$133,000	$1,565,623	**$1,698,623**
2014 *	$ 99,000	$ 924,398	**$1,023,398**

*Through July 2014

EXHIBIT 11

Source: Document Request Response 3-4

5.2 Transmission Physical Security Protection

NERC standards focus on the bulk electric system, which includes all transmission facilities that operate at 100 kV and above. The Florida Public Service Commission's jurisdiction includes all transmission assets 99 kV and below. Gulf operates transmission assets of 69 kV to 256 kV. The company operates 27 stand-alone transmission substations and 29 combined transmission and distribution substations. The company states its transmission substations are designed and maintained in accordance with applicable NERC standards and within the National Electrical Safety Code.

5.2.1 Risk and Vulnerability Assessments

In addition to analysis required by NERC CIP standards to identify transmission assets critical to the bulk electric system, Gulf management performs risk- and threat-based analyses to identify substations that the company deems to be critical to reliability. In 2013, to prepare for NERC CIP Version 5 implementation Corporate Security and Power Distribution management performed an updated risk-assessment of transmission assets. Key components to the asset assessments included:

- Threats (national, Southern Company, or location specific)
- Criminal Activity
- Historical/Previous Events
- Proximity to Law Enforcement
- Urban or Rural Location

- Current Security
- Criticality

From this risk-assessment, Gulf developed an internal *criticality* listing that captured more assets than the current NERC CIP standards criteria. With this listing, the company increased the number of facilities needing a higher level of protection from a physical security perspective.

For these critical assets, the company implemented a program to evaluate and analyze the security measures in place at each of these sites. These assessments were performed in the second quarter 2014, and the company is currently evaluating the results. For each facility, Corporate Security and Power Distribution management customized these assessments to include site-specific criteria. The company will use these assessments to determine whether additional security measures may be needed at each site.

For Gulf facilities identified as *critical* under NERC CIP standards, 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 "cube" (walls, ceiling, and floor) that houses the cyber asset. In most cases, the six-wall cube is either the control center or the control house building at a substation. These stations are required under NERC CIP standards to employ security measures above the company's baseline. This additional security would include such components as card readers, visitor logs, cameras, and video analytics.

For assets deemed non-critical, Gulf uses a baseline standard for securing substation perimeters that meets the requirements of the National Electrical Safety Code. The baseline standard specifies requirements for fencing with barbed wire capping and gate and door locks. At some substations, the company employs a higher level of physical protection, including, but not limited to: cameras, alarms, lighting, and key card assess. This additional protection is determined on a case-by-case basis, with input from both Corporate Security and Power Distribution management.

As advancements in video technology occur, Corporate Security and Power Distribution management assess and weigh the benefits of updating equipment. Gulf has incorporated camera monitoring technology in some of its substations that can differentiate between human and animal activity. All facilities equipped with cameras are monitored in the Gulf Security Control Center.

In Gulf's vulnerability assessment process, the company monitors and tracks security-related incidents at its substations. As shown in **Exhibit 12**, for the period 2010 through mid 2014, the company's 27 stand-alone transmission substations, Gulf recorded six substation incidents. The company notes all of these were a result of theft of materials located within the substation perimeter.

Gulf Power Company Transmission Substation Security Incidents 2011-2014					
Types of Incidents	**2011**	**2012**	**2013**	**2014***	**Total**
Intrusions of Fenced Perimeter/Trespassing	1	0	0	0	**0**
Intrusion-Theft	1	2	2	0	**6**
Intrusion-Destruction of Equipment or Property	0	0	0	0	**0**
Vandalism/Suspicious Activity	0	0	0	0	**0**
Total	**2**	**2**	**2**	**0**	**6**

*Through July 2014

EXHIBIT 12

Source: Document Request Response 4.1

As **Exhibit 13** shows, at its 29 combined transmission/distribution substations the company recorded ten substation incidents for the period 2011 through June 2014. Of these, eight were theft, one was suspicious activity, and one was intrusion or trespassing with no sign of theft.

Gulf Power Company Combination Substation Security Incidents 2011-2014					
Types of Incidents	**2011**	**2012**	**2013**	**2014***	**Total**
Intrusions of Fenced Perimeter/Trespassing	0	1	0	0	**1**
Intrusion-Theft	3	4	0	0	**7**
Intrusion-Destruction of Equipment or Property	0	0	0	0	**0**
Vandalism/Suspicious Activity	0	1	0	0	**1**
Total	**3**	**6**	**0**	**0**	**9**

*Through July 2014

EXHIBIT 13

Source: Document Request Response 4.1

5.2.2 Physical Security Inspection Process

In addition to the assessments performed on the identified "critical" transmission assets referenced above, the company conducts annual inspections on all of its transmission substations. These are visual and walk-through inspections of substation property and equipment. Security components monitored include fencing and gate maintenance, vegetation growth, and lock maintenance. These inspections provide a record of the facility's status, and note whether any adjustments are required. From 2013 through the first six-months of 2014, the company completed 30 transmission substation inspections.

5.3 Distribution Physical Security Protection

As noted, Gulf's distribution and transmission facilities up to 99kV are under the jurisdiction of the Public Service Commission for reliability and safety. Distribution substations

are connected to the transmission system and the voltage is stepped-down to a level appropriate for customer distribution. Currently, Gulf has 74 stand-alone distribution substations.

5.3.1 Risk and Vulnerability Assessments

Gulf management states the company does not differentiate its approach to physical security between transmission and distribution assets. Rather, all significant assets are afforded a risk-based site-specific threat assessment. The company determined that no stand-alone distribution substation met its criteria as critical during the most recent risk-assessment process. The company notes that most distribution substations are served from the company's networked transmission system, allowing service to be restored via a redundant or alternate source with minimum reliability impact.

Corporate Security notes that the threats to distribution substations are theft and vandalism, which can pose a safety hazard to the perpetrators. As with transmission substations, the company reviews distribution substation vulnerability on a case-by-case basis, and additional security measures are added to the site as needed.

As with transmission, the company employs a baseline standard for securing the perimeter of its distribution substations. The standard must meet the National Electrical Safety Code, however Gulf management states the company will employ a higher level of physical protection for distribution substations where determined appropriate. The company notes that no distribution substations fall under current or proposed NERC CIP requirements.

Gulf monitors incidents at its stand-alone distribution substations for trending and assessing vulnerability. For the period 2011 through July 2014, Gulf recorded 15 incidents at its 74 distribution substations. Of these, 12 were intrusion with theft of equipment or supplies, two were intrusion or trespassing with no sign of theft, and one was vandalism of the site. **Exhibit 14** details the number of incidents by year.

Gulf Power Company
Distribution Substation Security Incidents
2011-2014

Types of Incidents	2011	2012	2013	2014*	Total
Intrusions of Fenced Perimeter/Trespassing	1	0	1	0	2
Intrusion-Theft	2	7	3	1	13
Intrusion-Destruction of Equipment or Property	0	0	0	0	0
Vandalism/ Suspicious Activity	0	0	1	0	1
Total	3	7	5	1	16

*Through July 2014

EXHIBIT 14

Source: Data Request 4.1

5.3.2 Physical Security Inspection Process

The company performs annual inspections of all distribution substations using the same inspection evaluation tools and criteria used for transmission substation inspections. Inspections are documented in the same manner and any identified issues are addressed by the business unit. From 2013 through the first six-months of 2014, the company completed 95 inspections of its distribution substations.

5.4 Recovery and Response

Southern Company's Business Assurance Council is charged with managing a corporate-wide program to enhance the resiliency of the company's overall business infrastructure, including areas of security One focus area under this program is infrastructure protection through business continuity and incident response. *Gulf Power Business Assurance Policy* requires each business unit—with business critical functionality— to develop a business recovery plan and Gulf is in the process of developing a contingency model for each of its business units.

Gulf has developed a *Business Recovery Plan* for its transmission system operations and control center. This document incorporates many of Gulf's security policies and procedures. The company anticipates the approval of this document by the end of 2014. For Power Distribution, the *Power Delivery Business Continuity Plan* incorporates components of the company's storm restoration model.

Due to its criticality, the physical security of the company's Transmission Control Center falls under NERC CIP requirements. The company maintains the physical security in accordance with NERC CIP-002 and CIP-006. The company's Distribution Control Center serves as the fully-functional emergency back-up for the Transmission Control Center. As such, the Distribution Control Center is subject to the same NERC CIP standards. The company is audited by the regional agency SERC on compliance at least every three years.

Gulf relies on the Southern Company Power Coordination Center, located in Alabama, for certain transmission control functions. This center can serve as an additional back-up for the Gulf Control Center, if necessary. The Southern Company facility is also subject to NERC CIP standards and is audited by SERC accordingly. Gulf management notes that necessary redundancies are incorporated in its communication structure between all control centers.

An additional component of the company's response plan is its participation with other Southern Company utilities in sharing key spare assets. Also, Gulf is a participant in the NERC Spare Equipment Database and the Edison Electric Institute Spare Transformer Equipment Program. These partnerships allow Gulf, in the event of a key asset failure, to locate and take possession of replacement equipment.

The complete loss of a distribution substation not only has limited impact of Gulf's system, but it is an infrequent event. Gulf states that total distribution substation outages are usually triggered by line faults and other secondary issues outside the substation facility. For the review period 2011 through 2014, the company reported 137 total distribution substation outages due to these secondary line operation issues.

The company reports 39 instances of complete loss of a distribution substation for this period due to events occurring within the substation. The majority of these events were attributed to animal intrusion or equipment malfunction. There were no instances of a complete substation outage due to vandalism or sabotage during this period. The company also notes that for all its unplanned substation outages, the majority were offline for less than five minutes per event. **Exhibit 15** lists the number of outages for the period.

Gulf experienced no unplanned total transmission substation outage events during the 2010-2014 review period.

Gulf Power Company Distribution Substation Unplanned Outages* 2011-2014			
Year	Distribution Substation Outages - Line Operation	Distribution Substation Outage-Substation Event	Total Distribution Substation Outages
2011	30	9	39
2012	50	16	66
2013	32	4	36
2014**	25	10	35
Total	137	39	176

*Excludes all weather-related outages for the period
**Through August 2014

EXHIBIT 15

Source: Document Request Response 4.10

5.5 CIP-014 Preparations

Management states it evaluated and analyzed the events surrounding the 2013 PG&E Metcalf substation attack. Through this analysis, Gulf and Southern Company identified several areas where the company could make improvements in its security approach. These included the need for improving relationships with local, state, and federal law enforcement; incorporating training and information sharing with law enforcement; needing to maintain or exceed the current NESC fencing standards; and executing a security approach that looks beyond the current security perimeters.

With NERC's CIP-014 final approval in November 2014, the company is evaluating its potential impact on the current approach to physical transmission asset security. As a member of the "Southern Seven" utilities (seven large IOUs in the Southeastern region), Gulf shares best practices and incident information among its regional utilities. This group is assessing NERC CIP-0014 and how the utilities must adjust their practices to comply.

Due to timing, Gulf has not yet implemented specific changes to its physical substation security process as a result of the new NERC CIP-0014 standard. However, the company notes that several of its recently implemented initiatives will assist in supporting the new requirements. Examples include the company's new Grid Watch program, its Law Enforcement Training initiative, and a centralized monitoring approach for its critical assets.

5.6 Self-Assessments and Exercises

Southern Company and Gulf were observers to the 2011 national GridEx exercise. In 2013, the Company was a full participant in the follow-up GridEx II event. This event included physical security and cyber readiness scenarios. Southern Company and Gulf state they incorporated lessons-learned by reviewing and modifying restoration plans, reviewing the threat

level process, and evaluating communication tools. The company plans to continue its participation in the upcoming GridEx III event planned for November 2015.

In addition to participating in national security drills, Gulf and Southern Company conduct a series of internal self-assessments to evaluate the utilities response to cyber and physical security events. These drills are required under the company's Business Assurance plan. Emergency response exercises are conducted at both the company and corporate levels. For the last three exercises, Gulf states that the company included federal agencies along with state and local law enforcement in its security drills.

6.0 Tampa Electric Company

6.1 Security Management

6.1.1 Security Organization

Tampa Electric Company's (TEC) physical security and emergency management operations are organized under the Corporate Physical Security and Emergency Management Department of its parent, TECO Energy, Incorporated (TECO). The department is headed by the Director of Corporate Security and Emergency Management, and is responsible for implementing the *TECO Physical Security Emergency Contingency Response Plan*.

The Director of Emergency Management and Business Continuity reports to the Director of Corporate Physical Security and Emergency Management, and is responsible for emergency preparedness and business continuity planning and implementation of the *TECO Emergency Contingency Response and Business Continuity Plan*. This includes the development and coordination of system restoration logistics and resilience strategies and plans to minimize the impact of potential catastrophic events.

Both emergency preparedness and security plans use the TECO Energy Incident Command System to respond to natural and other disasters. The system provides coordination between different levels of internal and external command and control responding to security and emergency threats and events. Most emergency events also have security impacts that rely on a coordinated security response by TECO, law enforcement, and emergency response agencies. The Incident Command System ensures emergency agencies are informed of the threat or disaster, establishes command and control responsibility, and coordinates communication between TECO and public emergency and law enforcement resources.

Corporate Physical Security is headed by the Director of Corporate Security and Emergency Management, and is responsible for:

- Conducting security investigations
- Coordinating security operations
- Managing and directing security and guard service contractors
- Providing oversight of the TECO central monitoring station

The central monitoring station provides 24 hour monitoring and surveillance of TECO facilities and assets, including generation stations, transmission and distribution control centers, transmission and distribution substations, buildings and other facilities. The central monitoring station dispatches TECO security personnel for emergency assistance and requests additional law enforcement resources when necessary.

After studying the Pacific Gas and Electric Metcalf substation attack, the Corporate Physical Security and Emergency Management Department added a Physical and Cyber Security Coordinating Team to its organization. This team monitors information related to physical and cyber security and stays abreast of changing legislation, rules, compliance issues, and trends impacting those fields. The team consists of representatives from all areas of the company and provides input to the Director of Corporate Security and Emergency Management regarding intelligence and regulatory issues. The Director of Corporate Security and

Emergency Management makes quarterly presentations to TECO officers regarding the *Physical Security Plan* status, industry trends, and current security issues.

6.1.2 Physical Security Policies and Plans

TECO Corporate Policy Number 3.03 addresses the protection of assets and prevention of losses due to unlawful acts. The Corporate Security Department implements this policy. The *Physical Security Plan* documents company actions and activities to ensure employee safety and to prevent the destruction of company property, facilities, and assets.

TECO's *Emergency Management and Business Contingency Plan* includes a series of emergency and security programs and plans (Annex Plans) aimed at preparing for and responding to catastrophic events. Each Annex Plan is a free-standing plan, assigning specific responsibilities, actions, and interactions to be completed during a catastrophic event. These Annex Plans are discussed with senior TECO management through the quarterly presentations by emergency and physical security management. The plans are tested annually through preparedness exercises and against mock events and scenarios.

There are eight types of Business Disruptions covered by TECO Annex Plans:

- Physical Security Emergencies
- Safety Emergencies
- Environmental Emergencies
- Energy Management Emergencies
- Natural Emergencies
- Cyber Security Emergencies
- Telecom Emergencies
- Facility Emergencies

The *Physical Security Plan* includes categorization of Bulk Electrical System cyber systems, required by CIP-002. It also provides for physical security protection of Bulk Electrical System cyber systems critical infrastructure, as required by CIP-006. The *Physical Security Plan* is integrated with other corporate plans and reviewed by the TECO Corporate Security and Emergency Management Department annually. The plan is reviewed internally by qualified TECO security professionals and updated as necessary.

TECO governs its compliance with Federal Energy Regulatory Commission rules and regulations through its Internal Compliance Program. The program is managed under the supervision and oversight of the TECO Energy Corporate Ethics and Compliance department. The Chief Ethics Officer is responsible for ensuring the prevention and detection of violations of applicable laws, regulations, and ethical guidelines. Compliance issues are reported to senior management and the Corporate Compliance Officer for resolution.

6.1.3 Interactions with Law Enforcement and Federal Agencies

TECO has established relationships with local, county, state, and federal law enforcement, and can draw upon these resources when security threats are exposed. Threat preparations are tested through periodic exercises and coordinated response events to simulate actual threats. The company has developed beneficial relationships within U.S. Department of Homeland Security, the Industrial Control Systems Cyber Emergency Response team, the National Cybersecurity and Communications Integration Center, local FBI offices, the Department of Energy and research laboratories at Idaho and Washington, and the Electric

Sector Information Sharing Advisory Center. These relationships contribute to keeping the company abreast of current physical and cyber threats and technologies to address them.

The Corporate Physical Security and Emergency Management Department also emphasizes the importance of threat and information sharing and the value of collaboration with law enforcement and government agencies. TECO is involved in the Regional Fusion Center, which is managed by the City of Tampa Police Department Urban Area Security Initiative. Members of the Regional Fusion Center, along with the Florida Department of Law Enforcement and TECO, plan and coordinate security events and exchange threat intelligence information.

TECO and TEC actively participate in conference calls hosted by industry trade associations such as the Edison Electric Institute and the North American Transmission Forum. These calls provide valuable insights to promote efficient use of utility resources in benchmarking, human performance measurement, applicable operating experience, physical and cyber security, and continuous improvement analysis and evaluation.

6.1.4 Physical Security Cost Tracking

TECO Corporate Physical Security works hand-in-hand with its internal business-unit partners to ensure appropriate security protection is implemented. However, due to current accounting methods, the total costs of physical security expenditures are not readily consolidated.

Capital security expenditures are included within *project site* costs, rather than separately allocated as *physical security* costs. Security costs for fences, gates, locks, cameras, and card entry equipment are initially charged as part of the capital project. Ongoing security equipment repair on the project site is charged as operations and maintenance expenses to the site incurring the cost. Therefore, those costs cannot be readily compiled to show the total costs of physical security.

Exhibit 16 shows the total annual budgeted security expenditures for TEC during the period 2011-2014, separated into Capital and Operation and Maintenance categories.

Tampa Electric Company
Corporate Security Budget
2011 – 2014

Year	Capital	Operations and Maintenance	Total
2011	$80,000	$4,647,000	**$4,727,000**
2012	$50,000	$4,763,000	**$4,813,000**
2013	$50,000	$4,874,000	**$4,924,000**
2014	$60,000	$4,744,000	**$4,804,000**

EXHIBIT 16

Source: Document Request Response 4-9

As shown by the chart, the Operations and Maintenance budget represents approximately 99 percent of the total TEC Security Budget dollars during the period reviewed. TECO tracks expenditures for armed Anti-Terrorism Officers, Risk Management Officers, unarmed guards, and the 24 hour operation of the TECO Central Monitoring Station. Company documents show that Guard Services totaled approximately $2.7 million during the period 2011 through 2014, and ranged between $630,113 and $706,792 annually. Other than guard

services, physical security costs applying to transmission substations, distribution substations, and control centers are included within the internal business-unit budget.

6.2 Transmission Physical Security Protection

TEC currently operates 67 transmission substations throughout its service territory. Transmission facilities are integrated with the Bulk Electrical System primarily at the 230 kilovolt (kV) level. TEC has no 500 kV transmission substations operating in Florida. The greatest number of TEC transmission substations operates at the 69 kV level. TEC also operates three transmission stations at its generating facilities. The company uses enhanced security packages, including armed guard patrols to protect critical transmission infrastructure, and customizes security packages for other substations.

6.2.1 Risk and Vulnerability Assessments

TECO has completed risk-based assessments to identify transmission facilities critical to the Bulk Electrical System, as required by CIP-002. TECO physical security for CIP-related transmission control centers, transmission stations and substations, is designed around the specific perceived risk for each facility and includes perimeter, facility, and building protections.

The Physical Security Perimeter and Electronic Security Perimeter are highly safeguarded at main control centers and power stations. TEC has armed guards at these critical locations to supplement other protections, including, gates, fences, locks, concrete barriers, card locks, cameras, and card access equipment.

TECO and TEC conduct facility walk-throughs and use industry accepted risk assessment methodologies to identify threats and hazards. Risk and vulnerability assessments consider the criticality of each facility to the Bulk Electric System and the potential impact if it is inoperable. TEC implements protection packages based on the critical nature of the asset, system impact if loss occurs, potential threat risks, and other criteria.

One additional piece of information considered in risk assessment is the number of security incidents reported at each facility. **Exhibit 17** shows the total number of transmission incidents experienced annually by TEC during the period 2011-2014.

Tampa Electric Company
Transmission Substation Security Incidents
2011-2014

Types of Incidents	2011	2012	2013	2014*	Total
Intrusions of fenced perimeter	3	1	-	-	4
Theft	7	9	1	1	18
Destruction of equipment or property	-	-	-	-	-
Vandalism	6	3	-	-	9
Total	16	13	1	1	31

* Through September 2014

EXHIBIT 17

Source: Document Request Response 4-5

The exhibit shows that TEC had a total of 31 security incidents at its 67 transmission substations during the period reviewed. The greatest number of security incidents were categorized as thefts and vandalism. The total number of TEC transmission incidents decreased to one each during 2013 and 2014 through September.

6.2.2 Physical Security Inspection Process

According to the company, the North American Electric Reliability Corporation does not currently require ongoing site specific physical security surveys of transmission substations and control facilities to ensure compliance with standards. However, TEC completed one site-specific physical security survey for a critical power station and for the transmission substation associated with it. TEC believes that CIP-014 standards may require additional site-specific physical security surveys for primary control centers and for certain transmission substations. It is also possible that the scope of the already completed physical security survey may be expanded by the standard. Therefore, TEC will complete these surveys after CIP-014 goes into effect.

Although the Corporate Physical Security and Emergency Management Department do not routinely complete site-specific physical security surveys of substations and control facilities, TEC Substation Operations personnel inspect transmission substations at least annually. Transmission substation inspections review each facility to ensure that assets are in proper operational condition. These scheduled inspections review the condition of substation facilities including: landscape, gates, fences, locks, ground wires, control building access, control cabinet, lightning arrestors, transformers, security lighting, signs, operating instructions, fuses, relays, and any abnormal conditions. Inspections are in accordance with the Substation Inspection Policy and are documented and stored in the Cascade system for results tracking and trending. The inspection policy outlines requirements for completing both transmission and distribution substation inspections.

Other less formal substation inspections are completed as part of ongoing substation work. Substation Operations personnel often visit substations to perform work. Before entering substations to perform work activity, team members are required to complete visual inspections. These inspections are not formally documented. Any abnormal conditions are reported to supervisory management for correction. Weekly security and operational performance inspections are also completed at high priority transmission substations located at TEC generation facilities.

6.3 Distribution Physical Security Protection

TEC currently operates 148 distribution substations throughout its service territory. Of the total number of distribution substations, 144 are 69kV and 4 are 138kV sized substations. For distribution substations, the company uses standard security protection packages conforming to Section 11 of the National Electrical Safety Code. TEC standard distribution physical security includes seven foot barbed wire topped chain link fences, gates, locks, control room doors and locks, lighting, and signage. Security enhancements are made where customized protection is required in response to instances of theft, vandalism, and intrusion.

6.3.1 Risk and Vulnerability Assessments

TEC states that its risk assessments for distribution substations indicate distribution substations are a less attractive target for attack because of limited customer impact and low

probability for a cascading event. Risk and vulnerability assessments are conducted for distribution substations when changes occur in:

- Size and make-up of the substation
- Surrounding environment conditions
- Threat risks
- Building codes
- Regulatory policy

An important consideration in TEC risk assessments is the number of security incidents reported at each facility being assessed. **Exhibit 18** shows the total number of distribution security incidents experienced annually by TEC during the period 2011-2014. The exhibit shows that TEC had 20 total distribution security incidents during the period. The greatest number of security incidents were categorized as thefts and vandalism. The total number of TEC distribution incidents decreased to one during 2013 and zero in 2014.

TAMPA ELECTRIC COMPANY
DISTRIBUTION SUBSTATION SECURITY INCIDENTS
2011-2014

Types of Incidents	2011	2012	2013	2014**	Total
Intrusions of fenced perimeter	3	-	-	-	3
Theft	7	5	-	-	12
Destruction of equipment or property	-	-	-	-	-
Vandalism	3	1	1	-	5
Total	13	6	1	-	20

** Through September 2014

EXHIBIT 18

Source: Document Request Response 4-6

6.3.2 PHYSICAL SECURITY INSPECTION PROCESS

The TECO Corporate Physical Security and Emergency Management Department does not routinely complete site-specific physical security surveys of distribution substations and control facilities. However, TEC's Substation Inspection Policy requires that all distribution substations are inspected at least annually to ensure that fences and locks are intact, relay control room doors are locked and secure, and that substation equipment is intact. The inspection policy outlines requirements for completing both transmission and distribution substation inspections.

Substation Operations personnel perform scheduled annual distribution substation facility inspections, examining the condition of substation facilities including: landscape, gates, fences, locks, ground wires, control building access, control cabinet, lightning arrestors, transformers, security lighting, signs, operating instructions, fuses, relays, and any abnormal conditions. These scheduled inspections are documented and stored in the Cascade system for results tracking and trending.

Less formal substation inspections are also completed as part of ongoing substation work. Before entering substations to perform work activity, Substation Operations team members are required to complete visual inspections. These inspections are not formally

documented. However, any abnormal conditions are reported to supervisory management for correction.

6.4 Recovery and Response

TEC participates in the *FRCC Generating Capacity Plan* adopted by the Florida Public Service Commission per Rule 25-6.0183. The plan provides detailed coordinated actions among electric utilities and state and local agencies. It also enables TEC to cope with a generating capacity shortage on its system and mitigate the impact of the emergency.

TEC also has established emergency preparedness plans that direct control center personnel in restoring transmission and distribution service from catastrophic events. The company conducts annual drills to ensure that if such events occur, they are managed successfully.

The TEC *System Restoration Plan* specifically details the process to restore TEC's system from a total outage event. It describes the necessary steps to bring the system back online, working with the Florida Reliability Coordinating Council Reliability Coordinator. In the case of a single transmission or distribution station being restored, switching instructions describe how to effectively restore the compromised station without introducing risk to the grid. These smaller recovery events are completed between the control center operator and field staff using three-way communications.

Exhibit 19 shows the number of transmission and distribution substation outages experienced during the period 2011-2014, excluding planned outages and outages caused by named storms. As shown in the exhibit, total transmission and distribution outages were their highest in 2011 and have trended lower since.

Tampa Electric Company
Transmission and Distribution Substation
Unplanned Outages*
2011-2014

Year	Transmission Outages	Distribution Outages	Total Outages
2011	34	157	**191**
2012	21	125	**146**
2013	12	160	**172**
2014**	36	69	**105**
Total	**103**	**511**	**614**

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

EXHIBIT 19

Source: Document Request Response 4-11

TEC operates its transmission and distribution system using redundancy and switching to resolve most outages and supply issues. It maintains critical spare transmission and distribution equipment to facilitate system restoration and resiliency. TEC also participates in the Edison Electric Institute Spare Transformer Equipment Program. The program provides for the sharing of large transmission transformers, which are expensive to stock and difficult to

transport. A catastrophic loss triggers the use of this nation-wide spare parts inventory to minimize the length of outages. After the PG&E Metcalf attack, a request was issued for spare transmission transformer radiators to help restore the substation.

6.5 CIP-014 Preparations

TEC participated in the North American Electric Reliability Corporation standard development process that produced the version of CIP-014 filed for approval with the Federal Energy Regulatory Commission on May 23, 2014. The CIP-014 standard received final approval from the Federal Energy Regulatory Commission on November 20, 2014.

The scope of NERC CIP-014, Physical Security standard is limited to transmission stations and substations, and to primary control centers for critical transmission stations and substations. The standard requires that a risk assessment for identification of *critical* transmission facilities, an evaluation of physical threats, and the development of a physical security plan be completed. After completing the assessment and evaluation, a qualified third-party must review the assessment. Similarly, a qualified third-party must then review the physical security plan.

Physical Security risk to transmission substations is managed through TECO's Physical Security Plan. TECO states that the Physical Security Plan will be revised in the near term to reflect changes in procedures and processes necessary to implement the new NERC CIP-014 regulatory requirements. TEC is assessing potential qualified third-party reviewers for the assessments and security plan to comply with CIP-014.

The company has identified preliminary dollar amounts for 2015 physical security improvements to comply with CIP-014, and to better protect against risks such as the PG&E Metcalf attack. The company has budgeted $500,000 for CIP-014 related improvements in 2015, and will determine the appropriate budget amounts beyond 2015 once the CIP-014 final standard requirements begin implementation. TEC believes CIP-014 requirements should not necessarily be extended to apply to distribution substation and system physical security.

6.6 Self-Assessments And Exercises

In preparation for the Republican National Convention during 2012, TECO completed a consequence management exercise with the City of Tampa and local, state, and federal law enforcement and emergency officials. This exercise was valuable in preparing the company for potential security and emergency scenarios prior to the convention.

TECO also completed two "Black Swan" table top exercises during 2012. Black Swan events are highly unpredictable, rare, and high impact scenarios, generally outside the normal frame of reference or experience. These types of exercises test TECO's ability to respond in emergency conditions to extraordinary events, and assist in identifying gaps in physical and cyber security and communication.

The TECO *Physical Security Plan* is tested annually through several different types of mock exercises. TEC actively participates in the North American Electric Reliability Corporation GridEx cyber security exercises to test and improve physical and cyber security. GridEx

exercises also help identify communication gaps where mitigation and improvement efforts may be directed.

TEC participated in both the 2011 and 2013 GridEx and GridEx II exercises. In 2013, TEC was a full player and exercise design team member. This allowed TEC to insert additional scenarios into the exercise to test the preparedness of utilities involved in the exercise. TEC noted that the GridEx exercises are an important part of its emergency preparedness and security programs. TEC expects to participate in the NERC GridEx exercise scheduled during 2015.

During GridEx and other role play exercises and drills, TEC tests both its cyber and physical security by using blended attacks to evaluate systems integrity, response, and resiliency. A blended attack is a cyber attack that exploits and assaults security flaws within a computer system or application. Any gaps found as a result of GridEx and other exercises are reviewed, assessed, and prioritized for planned mitigation.

7.0 Appendices

Appendix 1 Physical Security Incidents 2010-2014

A limited number of physical attacks on substations nationwide have occurred over the last five years. This list represents a comprehensive but possibly not extensive list of these attacks. Included are attempts to cause serious operational disruption as well as incidents that may point to potentially significant breaches regardless of success. Note that the dates are based on media coverage reports and may not exactly match the date of incident.

Date	Location	Description
August 28, 2014	San Jose, CA	*PG&E Metcalf Ssubstation Theft.* Thieves cut through a fence and stole equipment. Unlike in 2013, this second incident at the same PG&E transmission substation did not seem intended to disable the facility.
June 11, 2014	Nogales, AZ	*Bomb planted at substation.* Makeshift bomb left under a diesel tank at transmission substation owned by UniSource Energy Services. Bomb did not explode but did ignite small fire. Service was not affected.
February, 2014	Watertown, SD	*Motor-operated switch shot at substation.* East River's Ortley substation motor-operated switch was shot 15 times. No service outages or interruptions; substation sustained $7,000 in damages.
October, 2013	Iroquois County, IL	*Vandal damage.* Eastern Illinois Electric Cooperative substation vandalized. Person(s) damaged the exterior and interior of a building.
August - October, 2013	Cabot, AR	*Series of attacks on transmission lines.* A major transmission line was attacked by person(s) attaching a cable to the framework of a 100-foot tower and across the railroad track. Bolts were removed from the base of the tower, but the effort failed to bring down the tower.
September 26, 2013	Keo, AR	*Fire at Keo substation.* Entergy Arkansas' control house was destroyed by arson, no injuries or power outages resulted. Vandals' message at site read, "YOU SHOULD HAVE EXPECTED U.S."
October 6, 2013	Lonoke County, AR	*Two power poles intentionally cut.* Two utility poles were cut down using a stolen SkyTrim tractor. The power lines targeted in the attacks link a high-voltage transmission line with a switching station or substation. The incident resulted in a power outage.
August 26, 2013	Lake Placid, FL	*Fire damage.* Glades Electrical Cooperative's Highlands Park substation severely damaged due to fire likely caused by gunshots. 1,300 customers lost power.
April 16, 2013	San Jose, CA	*Attack on PG&E Metcalf substation.* Phone lines to transmission substation were cut. 17 large transformers damaged by rifle fire. No service interruption or outages. Substation sustained $15.4 million in damages and disabled for almost a month. FBI investigation ongoing. No service interruptions occurred.
December 16, 2012	Heber, AZ	*Transformer shot at substation.* Large power transformer at Navopache Electric Cooperative's substation shot multiple times, causing a 10-hour blackout in the Heber and Overgaard communities and surrounding areas.
September 7, 2012	Tahlequah, OK	*Substation shot by vandals.* Four shots from high-powered rifle caused $1 million in damage to Lake Region Electric Cooperative substation. Two shots hit main transformer and two hit electric circuit breakers resulting in 2,000 customers losing power for less than 2 hours.

Date	Location	Description
January 31, 2012	Little River, SC	*Vandalism of substation.* 4,500 customers lost service for six hours after attempted break-in at the Horry County Electric Cooperative substation. Specific details not released due to criminal investigation.
March 31, 2011	Gillette, WY	*Substation transformer shot at Powder River Energy Corp.* The vandalism caused more than 270 customers to lose power service.
July 5, 2010	Hamilton County, IL	*Oil drained from transformer.* Intruder(s) drained oil from a large transformer. Alarms at dispatch center alerted workers who remotely opened circuit breakers to prevent transformer from overheating and possibly exploding.

Source: Energy Sector Security Consortium, Inc.: A Summary of Physical Substation Incidents 2010-2014

Appendix 2 NERC Physical Security Response Guidelines

The NERC physical security response guidelines suggest activities that are appropriate for each of the three threat alert status ratings issued by the United States Department of Homeland Security (normal risk, elevated risk, imminent risk). For each level of increased threat alert, increasingly stringent preparedness and response activities are suggested. Adherence to these guidelines is voluntary. They are intended by NERC to provide a suggested framework for physical threat response by utilities.

Normal Operations Risk
1. Confirm normal security operating procedures are current, in place, and operational.
2. Provide training and updates for the security staff and key personnel on all aspects of the response plan, as well as pre-planned operating procedures.
3. Periodically issue workforce security awareness messages.
4. Train mail handling personnel and all employees handling mail directly on-site on characteristics of suspicious mail or packages. Review response procedures for these items.
5. Brief on timely and threat related security topics at employee meetings to increase security awareness.
6. Provide recurring training of hazardous material, security, and emergency response personnel.
7. No persons should be permitted access to the facility without proper authorization by authorized management.
8. Authorized persons will adhere to access control procedures and prevent tailgating or other unauthorized entry.
9. Identification badges, permanent or temporary are required for all individuals onsite, including employees, contractors, and visitors.
10. Individuals or persons not possessing or displaying an identification badge should be challenged to determine their identity and reason for their presence. Appropriate action should be taken upon this determination.
11. Visitors should receive visitors badges, be required to sign in, providing appropriate identification to verify their identity.
12. Annually audit electronic or other access programs for critical facilities to ensure proper access authorization.
13. Conduct routine maintenance and inspection of security equipment to ensure that it is in good working order.
14. Conduct routine security inspections, patrols of the facility and critical areas, and components and reports submitted of findings.
15. Conduct periodic security tabletop exercises with facility and/or executive management as appropriate. Consider involvement of law enforcement support as well as tour of facilities for familiarity of response.
16. Review and update all security, threat, cyber, business continuity, and disaster-recovery plans on an ongoing basis or at least once every year.
17. Unusual or suspicious activities observed by personnel should be reported to local law enforcement, local management and security.
18. Identify critical facility long-term and short-term security measures as appropriate. Examples of security measures are: • Electronic security systems (locks, alarms, cameras, access control, etc.) • Closing nonessential perimeter and internal portals • Identify and secure all essential perimeter and internal portals and establish accountability • Physical barriers such as bollards or concrete barriers • Perimeter signage • Fence integrity • Lighting effectiveness • Security surveys • Vulnerability assessments • Availability of security resources – contract and proprietary • Law enforcement liaison (FBI, jurisdictional law enforcement agencies, Fusion Center, etc.) • Maintain essential spare parts for critical facilities

Elevated Risk
19. Communicate the heightened alert level to all security staff and onsite personnel at the critical facilities. This should include vendors with routine deliveries. The communication should include a reminder to be alert for unusual or suspicious activities and to where it should be reported. Security staff at other, noncritical facilities also should be made aware of increased threat level.
20. Inform local law enforcement agencies that the facility is at an elevated alert level, confirm communications methods to be utilized and advise them of them of security measures being employed. Request that agencies increase the frequency of patrols at critical facilities.
21. Security personnel should review company security and incident response plans and procedures.
22. Review operational plans and procedures to ensure they adequately address the threat associated with the reason(s) for the elevated alert level. They should include the following: • Security, threat, disaster recovery, fail-over plans, and business continuity plans • Other operation plans as appropriate, e.g., transmission control procedures • Availability of additional security personnel • Availability of medical emergency personnel • Review of all data and voice communications channels to assure operability, user familiarity, and backups function as designed • Review of fuel source requirements • Review vehicle search procedures.
23. Limit facility access to required visitors, personnel, and vehicles.
24. Increase surveillance of critical areas and facilities.
25. Monitor and restrict all deliveries. Particularly deliveries of combustible materials such as startup fuel, diesel fuel, and gasoline. Confirm delivery with receiving personnel. Request list(s) of anticipated deliveries of those essential to continued operations.
26. Verify the identity of delivery personnel and conduct a general inspection of deliveries, if feasible, (for example, verify that paperwork is in order and the external appearance of deliveries is consistent with the paperwork)
27. Conduct random inspections of vehicles, bags, backpacks, purses, etc.
28. Ensure all gates, security doors, and security monitors are in working order, and that visitor, contractor, and employee access controls are enforced.
29. Evaluate the necessity of non-vital maintenance and capital project work that could affect facility security. Delay or reschedule this work as appropriate.
30. Increase lighting in facility buffer zones, if feasible.
31. Establish and assure ongoing internal and external communications and coordinate the organization's action plan with local, state/provincial, and federal law enforcement agencies as appropriate.
32. Verify the operating condition of all security systems such as detectors, monitors, intruder alarm systems, and lighting upon receipt of an elevated threat advisory, and weekly thereafter until termination of the advisory.
33. Increase monitoring of network intrusion systems.
34. Identify additional business- and site-specific measures as appropriate.
35. Remind personnel of the reporting requirements for any unusual enterprise or control systems network activity and to be vigilant regarding suspicious electronic mail.
36. Conduct security awareness briefings for employees and on-site contractors.
37. Coordinate the security of critical facilities with neighboring organizations including other electricity sub-sector organizations and large customers.
38. Use communications channels with local, state/provincial, and federal law enforcement agencies and other emergency management agencies responsible for responding to the critical facility to assess the nature of any threats to the facility or organization.
39. Place all essential critical facility support personnel on alert.
40. Consider deployment of additional security personnel if there is sufficient information to suggest a heightened probability of attack on the facility or the surrounding area.
41. Consider restricting parking around critical facilities and/or outside perimeter fence.
42. Where appropriate, ensure all gates and security doors are locked and actively monitored twenty-four hours a day, seven days a week, either electronically, or by random patrol procedures.
43. Enforce strict control of visitors and visitor vehicles entering critical facilities.
44. Consider postponing or canceling nonessential tours and visits.
45. When appropriate, contact suppliers and coordinate with combustible deliveries as necessary.
46. Perform a periodic inspection of site fuel storage and hazardous material facilities.
47. To the extent practical, coordinate critical facility security with adjacent facilities.

48. Consider making immediate repairs and return to service any essential equipment that is inoperable due to repair or maintenance. If possible, suspend scheduled maintenance for essential equipment.
49. Coordinate any security related media releases with security, media relations, and management.
50. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.
Imminent Risk
51. Communicate the heightened alert level to all on-site personnel. The communication should include a request to be alert for unusual or suspicious behaviors or activities and to whom such should be reported. Ensure all on-site personnel are fully briefed on emergency procedures and emergency conditions as they develop.
52. Contact local, state and provincial, federal law enforcement and other government agencies to determine nature of threat and applicability to operations. Establish frequent communications with all appropriate law enforcement agencies for two-way updates on threat status.
53. Unless conditions dictate otherwise, open emergency center(s).
54. Account for all personnel at affected locations.
55. Implement security, incident response and business continuity plans as needed.
56. Security Managers should review security personnel requirements and augment with qualified personnel.
57. Consider deployment additional security personnel and resources to critical facilities.
58. Consider release of nonessential personnel depending on the nature of the threat or incident.
59. Limit facility access to essential staff, visitors, and contractors.
60. Cancel or delay non-vital contractor work and services.
61. Allow deliveries from trusted vendors, contractors, suppliers by appointment only. Inspect all deliveries, to include packages and cargo. Require advance notice of deliveries and identification of drivers.
62. Inspect all bags, backpacks, purses, etc., prior to entering the facility.
63. Inspect all vehicles prior to gaining access to the facility.
64. Discontinue all tours and visitors.
65. Consider discontinuing mail and package deliveries to critical facilities or deliver to offsite locations for inspection or subsequent delivery.
66. Consider suspending maintenance work on essential equipment, except work that management determines to be emergency work and critical.
67. Continuously monitor or otherwise secure all entrances to critical service facilities. This step may include use of armed security personnel or law enforcement officers. Heavy equipment and storage material may be moved and used as barriers at closed entrances.
68. Erect barriers and/or obstacles to control vehicle traffic flow and protect the facility from attack by moving vehicles.
69. Identify and implement plans for any additional measures specific to facility as appropriate based on available intelligence.
70. If feasible, close public access areas such as boat ramps and recreation areas. If these facilities are part of projects licensed by the Federal Energy Regulatory Commission (FERC), inform the FERC regional office of the decision as soon as practical. Coordinate with local authorities regarding the closing of nearby public roads and facilities, if appropriate.
71. Where possible, restrict vehicle parking to 150 ft. from all critical areas and assets.
72. Limit network communications links to essential sites/users.
73. Review remote access for individuals and revoke any credentials that are not current and necessary.
74. Conduct daily security and awareness briefings for each shift relevant to security concerns of the alert or threat.
75. Participate in situation update briefings with government agencies, local law enforcement, and internal inter-dependent business units, as well as coordinate media releases or inquiries, and coordinate impacts to adjacent/nearby businesses or neighbors.
76. In the event of an actual incident affecting the Grid, Security Personnel should liaison with Grid Operations Personnel to ascertain the next potential affected site in the critical path.
77. Continue to monitor situation and be prepared to de-escalate to a lower threat alert level.

Source: North American Electric Reliability Corporation Security Guideline for the Electricity Sub-sector: Physical Security Response