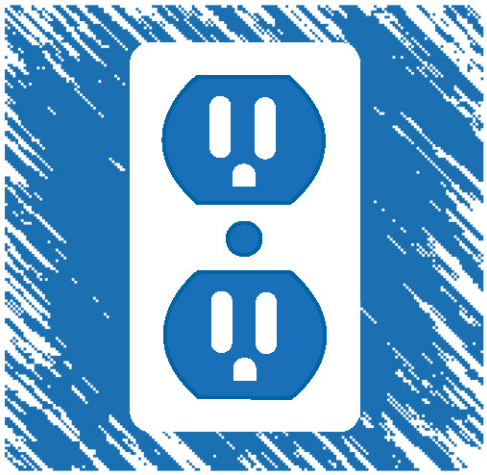


Review of Cyber and Physical Security Protection of Utility Substations and Control Centers

APRIL 2018

BY AUTHORITY OF

The Florida Public Service Commission
Office of Auditing and Performance Analysis

Review of Cyber and Physical Security Protection of Utility Substations and Control Centers

Jerry Hallenstein
Senior Analyst
Project Manager

David Rich
Public Utility Analyst IV

Sofia Lehmann
Public Utility Analyst II

Vic Cordiano
Engineering Specialist II

Bob Casey
Public Utility Analyst I

Melissa Hardison
Public Utility Analyst I

April 2018

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

PA-17-08-004

TABLE OF CONTENTS

TABLE OF EXHIBITS

1.0 Executive Summary

1.1 Purpose and Objectives

In 2014, the Florida Public Service Commission's (FPSC or Commission) Office of Auditing and Performance Analysis conducted a review of the physical security measures used to protect transmission and distribution substations, control centers, and associated cyber assets employed by four investor-owned electric utilities (IOUs) in Florida:

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

In its December 2014 audit report, Commission audit staff underscored the need for the Commission to keep abreast of efforts taken by Florida IOUs to prevent, detect, respond, and recover from cyber and physical attacks against their key system assets. The report observed that federal requirements have laid a solid foundation for protecting the most critical Bulk Electric System (BES) sector assets operated by Florida IOUs, while noting that these standards exclude most assets that fall within the Commission's jurisdiction. Audit staff expressed concerns about the cost of complying with critical infrastructure protection standards and noted that careful analysis of costs and risks is necessary to maintain a prudent level of investment in protections on behalf of ratepayers.

Commission audit staff initiated this follow-up review in August 2017 to examine and to report on the utilities' compliance activities, planning, and protection efforts over the period 2015 through 2017. This review includes an updated summary of the revised requirements for compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), Emergency Preparedness and Operations (EOP), and Transmission System Planning (TPL) reliability standards. These NERC reliability standards impose a comprehensive set of compliance requirements impacting system and facility design and operations. They are designed to better secure critical assets to ensure reliable operation of the BES.

The primary objectives of this review were met by reviewing and documenting each utility's:

- Development, implementation of internal controls, and compliance with Versions 5 and 6 of NERC CIP-002 through CIP-009 approved by Federal Energy Regulatory Commission (FERC) in November 2013 and January 2016, respectively;

- Development, implementation of internal controls, and compliance with Version 2 of NERC CIP-010 and CIP-011 approved by FERC in January 2016;

- Activities in anticipation of final approval by FERC of NERC CIP-012 and CIP-013, both of which are under development;

- Development, implementation of internal controls, and compliance with Version 2 of the physical security directives as prescribed in NERC CIP-014 and as approved by FERC in July 2015;

- Self-initiated actions or program participation to enhance cyber and physical security protections in addition to the NERC reliability standard requirements;

- Cyber and physical security incident reporting internal controls and compliance with NERC EOP reliability standards, DOE, and FPSC reporting obligations;

- Methods of identifying industrial control system (ICS) risks and proactively mitigating such threats;

- Compliance activities regarding NERC Emergency Preparedness and Operations (EOP) and Transmission System Planning (TPL) reliability standards;

- Safeguards voluntarily undertaken since 2014 to protect critical transmission and distribution assets against cyber and physical security threats;

- Updated changes since 2014 to internal organizations responsible for cyber and physical security oversight of company operations;

- Internal and external simulations, drills, and exercises conducted since 2014 to identify cyber and physical security improvements and to verify response and recovery readiness;

- Recent developments regarding cyber and physical security information sharing between utilities, industry associations, state and federal regulatory agencies, and law enforcement;

- Most recent NERC reliability standards compliance audits and internal audit review results, and approach to risk management through compliance monitoring and internal control activities; and

- Initiatives to separately track cyber and physical security costs.

1.2 Scope

Given these objectives, the scope of the review primarily focused on each company's current compliance efforts related to NERC's reliability standards and examined each company's plans to comply with new or changing requirements. Currently, all of the utilities' critical assets that impact the Bulk Electric System fall within the scope of compliance under NERC standards for cyber and physical security.

Commission audit staff further examined security protections in place for transmission and distribution assets that are not subject to the mandatory NERC standards, yet fall within the Commission's jurisdiction. The Commission has jurisdiction of transmission facilities below 100 kV and the distribution electrical system throughout Florida.

Commission audit staff also documented the utilities' interactions with other governmental and industry organizations and advisory groups that provide cyber and physical security oversight and assistance to the utilities.

Finally, the report documents the utilities' plans and preparations for reporting and recovering from cyber and physical security attacks.

1.3 Methodology

Planning, research, and data collection for this review were performed from August 2017 through February 2018. The information compiled in this document was gathered through responses to document requests and on-site interviews with key employees accountable for each utility's cyber and physical security plans, procedures, and operations. Specific information collected and reviewed from each utility includes:

- Physical security program policies, procedures, and processes;
- Substation and control center risk assessments and inspections;
- Audits or assessments conducted on the company's transmission and distribution operations by regulators and industry peer organizations;
- Occurrences of cyber and physical security incidents; and
- Documentation relating to participation in collaborative industry groups.

1.4 Audit Staff Observations

Through its review, Commission Audit Staff observed the following:

- Over the period 2015 through 2017, NERC implemented extensive revisions and additions to CIP and other reliability standards.
- The added NERC protective measures expanded some requirements previously imposed on High Impact and Medium Impact BES Cyber Systems to also cover Low Impact BES Cyber Systems.
- Florida IOUs dedicated significant effort and resources to compliance activities over the period 2015 through 2017.

- Independent of Federal regulatory requirements, Florida IOUs continue to assess necessary system protections through risk-based analysis to guide decision-making regarding investment in cyber and physical security protections.

- To date, no successful efforts to disrupt the U.S. Bulk Electric System have occurred.

- Efforts to disrupt critical infrastructure sectors of the U.S. economy by various categories of malicious actors continue to increase sharply.

- Both external and internal audits of cyber and physical security protections provide rigorous oversight of controls adequacy and regulatory compliance.

2.0 Background and Perspective

2.1 NERC Reliability Standards

In July 2006, the Federal Energy Regulatory Commission (FERC) certified North American Electric Reliability Corporation (NERC) to develop, monitor, and enforce compliance with its electric reliability standards. Under FERC Order Nos. 693 and 706, issued March 16, 2007 and January 18, 2008, all users, owners, and operators of the Bulk Electric System (BES) must comply with the NERC reliability standards. The BES is defined as all transmission elements and interconnections with neighboring systems operating at 100 kV and greater.

Over 100 NERC reliability standards exist regulating activities such as:

- Communications and coordination
- Emergency preparedness and operations
- Interconnection coordination and reliability operations
- Demand reporting and load management
- Transmission system planning
- Operating personnel responsibilities
- Critical infrastructure protection
- Nuclear plant interface coordination

Failure to comply with the requirements may trigger sizable penalties of as much as $1.2 million dollars per day per violation.

Subsequent to Commission audit staff's 2014 review, NERC adopted new and revised Critical Infrastructure Protection (CIP), Emergency Preparedness and Operations (EOP), and Transmission System Planning (TPL) reliability standards for the protection and security of critical cyber and physical assets supporting the BES. Critical cyber assets are any programmable electronic devices and communication networks including hardware, software, and data. Specific examples include Supervisory Control and Data Acquisition Systems (SCADA), Energy Management Systems (EMS), and Plant Distributed Control Systems (DCS). Examples of critical physical assets include generating resources, transmission stations and substations, and control centers.

2.1.1 Critical Infrastructure Protection (CIP) Reliability Standards

NERC has currently adopted 11 Critical Infrastructure Protection (CIP) reliability standards to protect the BES from cyber and physical attacks. These 11 CIP standards are further broken down into 167 cyber and physical security protection requirements that each utility must monitor and implement. The requirements include measures for identifying critical cyber assets, developing security management controls, training, perimeter and physical security, and using firewalls and other cyber security measures to block against cyber attacks.

Various NERC CIP standards require the creation of 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.

NERC uses a common organizational format for each CIP reliability standard that includes three primary sections: (a) Introduction, which includes the "Purpose" and "Applicability" sub-sections; (b) Requirements and Measures; and (c) Compliance, which includes a "Table of Compliance Elements". **Exhibit 1** provides a list of the 11 CIP reliability standards currently subject to NERC enforcement, the corresponding current version number approved by FERC, and the title and purpose of each CIP.

CIP Cyber Security Reliability Standard Revisions 2013-2018

The initial NERC CIP-002 through CIP-009 reliability standards were approved by FERC in January 2008. These standards have since been significantly revised. The transition from Version 3 to Version 5 in November 2013 represented a major change in requirements and approach. FERC authorized the direct transition to Version 5 allowing utilities to skip the interim CIP Version 4. Prior to Version 5, CIP standards applied to only the most critical BES assets and cyber systems as identified through risk-based assessments performed by owners and operators. As a result, a wide range of assets and cyber systems had few compliance obligations under the CIP standards.

In CIP Version 5, the most notable change is the addition of a tiered impact rating system which classifies BES critical assets and cyber systems into High, Medium, and Low Impact ratings based upon individual risk profiles. A High Impact facility is one whose importance necessitates greater protection than a Low Impact facility, based on likelihood of attack and severity of potential consequences. Version 5's new "bright-line" approach for identifying critical assets ensures that cyber systems at all BES facilities operating at or above 100 kV are within scope for at least some requirements and qualify for protection under the CIP standards.

An updated Version 6 of CIP-003, CIP-004, CIP-006, CIP-007, and CIP-009 was issued in January 2016 to add greater clarity in the requirements. Version 6 of CIP-003 specifically imposed new requirements for Low Impact BES Cyber Systems.

In addition to revisions of the initial CIP-002 through CIP-009 standards, FERC also approved Version 1 of CIP-010 and CIP-011 in November 2013 and most recently Version 2 in January 2016. CIP-010 Version 2 focuses on providing controls to address the risks posed by transient electronic devices such as USB flash drives. The primary focus of CIP-011 Version 2 is requiring an information protection program to prevent unauthorized access to BES cyber system information and dissemination upon reuse or disposal.

NERC Critical Infrastructure Reliability Standards			
Standard	**Version**	**Title**	**Purpose**
CIP-002	5	BES Cyber System Categorization	Identify and categorize BES cyber systems and their associated BES cyber assets.
CIP-003	6	Security Management Controls	Specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES cyber systems against compromise that could lead to misoperation or instability in the BES.
CIP-004	6	Personnel and Training	Require an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES cyber systems.
CIP-005	5	Electronic Security Perimeters	Manage electronic access to BES cyber systems by specifying a controlled electronic security perimeter in support of protecting BES cyber systems against compromise.
CIP-006	6	Physical Security of BES Cyber Systems	Manage physical access to BES cyber systems by specifying a physical security plan in support of protecting BES cyber systems against compromise.
CIP-007	6	System Security Management	Manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES cyber systems against compromise.
CIP-008	5	Incident Reporting and Response Planning	Mitigate the risk to the reliable operation of the BES as the result of a cyber security Incident by specifying incident response requirements.
CIP-009	6	Recovery Plans for BES Cyber Systems	Recover reliability functions performed by BES cyber systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
CIP-010	2	Configuration Change Management and Vulnerability	Prevent and detect unauthorized changes to BES cyber systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES cyber systems from compromise.
CIP-011	2	Information Protection	Prevent unauthorized access to BES cyber system information by specifying information protection requirements in support of protecting BES cyber systems against compromise.
CIP-014	2	Physical Security	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 instability, uncontrolled separation, or cascading outages within an interconnection.

Exhibit 1

Source: NERC Reliability Standards

CIP-014 Physical Security

The status and implementation of CIP-014 was a primary focus of Commission audit staff's 2014 report. The purpose of CIP-014 is to enhance the physical security measures for the most critical transmission stations, substations, and associated primary control centers in an effort to reduce the overall vulnerability against physical attacks. CIP-014 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 also at risk from malware and viruses. Utilities depend heavily on information technology to control many basic transmission and distribution functions.

CIP-014 had yet to be fully implemented by completion of Commission audit staff's 2014 audit report. At that time, the four IOUs included in this review were still in the analysis phase of the implementation of CIP-014. The analysis phase included site-by-site vulnerability assessments with the focus on threats, preventive measures, event mitigation, and event recovery. Each utility has since fully implemented physical security plans for their respective critical facilities. Key changes resulting from the implementation of CIP-014 are discussed further in the report chapters specific to each utility.

CIP Waiver During Exceptional Circumstances

NERC allows waiver of a particular CIP requirement under limited instances. NERC defines a CIP Exceptional Circumstance as a situation that involves or threatens to involve a risk of injury or death; a natural disaster; civil unrest; an imminent or existing failure of hardware, software, or equipment; a cybersecurity incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment to large scale workforce availability.

At the conclusion of the Exceptional Circumstance, cyber and/or physical security controls are restored as quickly as possible and compliance with all standards shall again be required. The Exceptional Circumstance is documented and approved by the CIP senior manager or delegates responsible for leading the adherence to these standards as soon as possible during or after the situation in accordance with NERC requirements.

Future CIP Reliability Standards

As of report publication, NERC was in the process of finalizing two new CIP reliability standards, CIP-012 and CIP-013. CIP-012 will require utilities to protect the confidentiality and integrity of real-time assessment and monitoring, and control data transmitted between control centers. CIP-013 will address security controls for supply chain risk management of BES cyber systems. It will require utilities to have plans in place that identify and assess cybersecurity risks to the BES from vendor products or services. In particular, the plans will address cyber security protections such as software integrity and authenticity, vendor remote access, information system planning, and vendor risk management and procurement controls.

2.1.2 Emergency Preparedness and Operations (EOP) Standards

Section 215 of the Federal Power Act required NERC to develop mandatory and enforceable Reliability Standards that are subject to FERC Commission review and approval. Emergency Preparedness and Operations (EOP) standards are NERC reliability standards which were approved by FERC. They address preparation for emergencies, necessary actions during emergencies, and system restoration and reporting following disturbances.

- EOP-004-3 (Event Reporting) improves the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

- EOP-005-2 (System Restoration from Blackstart Resources) ensures plans, facilities, and personnel are prepared to enable system restoration from blackstart resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

- EOP-006-2 (System Restoration Coordination) ensures plans are established and personnel are prepared to enable effective coordination of the system restoration process to ensure reliability is maintained during restoration and priority is placed on restoring the Interconnection.

- EOP-008-1 (Loss of Control Center Functionality) ensures continued reliable operations of the BES in the event that a control center becomes inoperable.

- EOP-010-1 (Geomagnetic Disturbance Operations) mitigates the effects of geomagnetic disturbance events by implementing operating plans, processes, and procedures.

- EOP-011-1 (Emergency Operations) addresses the effects of operating emergencies by ensuring each Transmission Operator and Balancing Authority has developed Operating Plans to mitigate operating emergencies, and that those plans are coordinated within a Reliability Coordinator Area.

2.1.3 Transmission System Planning (TPL) Standards

In May 2013, FERC directed NERC to develop reliability standards to address the potential impact of geomagnetic disturbances on the reliability operation of the BES. NERC created TPL reliability standards to ensure that transmission systems are planned and designed to meet a specific set of reliability criteria. The Standards address the types of simulations and assessments that must be performed to ensure that reliable systems are developed to meet present and future system needs. They provide information required to assess regional compliance with planning criteria and for self-assessment of regional reliability.

Geomagnetic Disturbance (GMD)

A GMD occurs when storms on the sun's surface produce electrically charged particles that interact with Earth's magnetic field. This could result in induced currents moving through transmission lines into transformers. During a GMD event, geomagnetically induced currents may cause transformer hot-spot heating or damage which may result in voltage collapse and blackout.

On September 22, 2016, FERC approved reliability standard TPL-007 to establish requirements for transmission system planned performance during GMD events. This standard addresses risks of voltage collapse and equipment damage in the BES caused by GMD events. In addition, FERC required that reliability standard TPL-007 be modified to reflect new information and analyses. It determined that additional collection and disclosure of geomagnetically-induced current monitoring and magnetometer data are necessary to improve the collective understanding of the threats posed by GMD events. FERC established a revision completion deadline of May 2018.

2.2 Notable Cyber and Physical Security Incidents

2.2.1 Physical Attack at Metcalf Substation (2013)

The physical attack on a Pacific Gas & Electric's Metcalf transmission substation near San Jose, California was detailed in Commission staff's 2014 report. Approximately 100 rounds of rifle fire under cover of darkness resulted in more than $15 million in damage to 17 transmission transformers. PG&E was able to avoid any customer outages by rerouting its power supply. After the attack, FERC imposed mandatory physical security standards for substations via the creation of CIP-014.

2.2.2 Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (2018)

On March 15, 2018, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) issued Joint Alert TA18-074A addressing Russian Government cyber activity targeting industries including the energy sector. The alert contains technical details on the tactics, techniques, and procedures used by Russian government cyber actors.

The DHS and the FBI reported that Russian government cyber actors staged malware, conducted spear phishing, and gained remote access into energy sector networks. They also state the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems.

Joint Alert TA18-074A includes detection and prevention guidelines and general best practices for utilities to help defend against this activity. The DHS offers incident response resources and technical assistance, and encourages companies who identify the use of tools or techniques discussed in this Joint Alert to report information to DHS or law enforcement immediately.

2.2.3 Industrial Control Systems Attack in Saudi Arabia (2017)

In December 2017, malicious software known as "Triton" was used to target critical safety and industrial control systems in Saudi Arabia. In the attack, perpetrators deployed malware designed to manipulate industrial safety systems. The targeted systems provide emergency shutdown capability for industrial processes. It is believed the attackers were developing a capability to cause physical damage and inadvertently shut down operations using an attack framework designed to interact with Triconex Safety Instrumented System controllers. Such controller systems provide remote computerized process control for companies in the energy, manufacturing, and mining sectors. Though not attributed to a specific threat actor the targeting of critical industrial infrastructure, a lack of monetary demands, and the use of highly technical resources required to create such a sophisticated attack profile may be consistent with a nation state actor.

Attackers gained remote access to at least one engineering workstation and deployed Triton to reprogram or manipulate the Safety Instrumented System controllers. As a result, some controllers entered a fail-safe state, automatically shutting down the industrial process and initiating an investigation. The investigation revealed that the controllers initiated a safe shutdown after a failed validation check. No damage was incurred.

2.2.4 Cyber Attack and Outages in Ukraine (2015)

In December 2015, hackers successfully compromised information and control systems at three Ukrainian state-owned electrical distribution utilities in the first cyber attack producing power outages. Thirty substations were remotely switched off by the attackers. Power was interrupted for approximately three hours system-wide and about 230,000 customers lost power for up to six hours. A fourth company was targeted but detected the system intrusion prior to the attack, underscoring the importance of effective controls and prevention efforts.

The attack consisted of a multi-phase operation over time that included:

- Spear phishing campaign to gain access and compromise corporate networks;
- Seizure of the SCADA, allowing attackers to remotely switch substations off;
- Disabling/destroying IT infrastructure components (e.g. uninterruptible power supplies);
- Destruction of files stored on servers and workstations; and,
- Call center disruption to deny consumers up-to-date information on the blackout.

While historically significant, this attack resulted in relatively minor customer impact, especially given the degree of effort expended, most likely by nation state actors. Though the systems targeted continue to operate in a degraded state two years after the event, all three utilities are able to serve their demand. Continued intrusion attempts followed into 2016 but none were successful in causing outages.

2.3 Florida Public Service Commission Oversight

2.3.1 Commission Rules and Jurisdiction

Chapter 366 of the Florida Statutes (F.S.) grants the Commission jurisdiction over subjects related to the cyber and physical security of the Florida electric utilities' infrastructure. Section 366.04(5), F.S. grants the Commission with the "jurisdiction over the planning, development, and maintenance of a coordinated electric power grid" assuring "an adequate and reliable source of energy for operational and emergency purposes in Florida and the avoidance of further 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."

Section 366.05(1), F.S., provides the Commission "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, for purposes of ensuring the reliable provision of service". The Commission also has the power to require "repairs, improvements, additions, replacements, and extensions to the plant and equipment of any public utility when reasonably necessary."

Under Section 366.05(8), F.S., the Commission has the power to require Florida electric utilities to install or repair any necessary facility "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, including inadequacies in fuel diversity or fuel supply reliability."

FPSC Chapter 25-6 of the Florida Administrative Code is intended "to define and promote good utility practices and procedures, adequate and efficient service to the public at reasonable costs, and to establish the rights and responsibilities of both the utility and the customer."

Florida's transmission system is comprised of lines rated at 69 kV, 115 kV, 138 kV, 230 kV, and 500 kV. NERC CIP standards are designed to protect the Bulk Electric System as discussed in Section 2.1. These standards exclude transmission facilities lower than 100 kV and the distribution system. However, the Commission has jurisdiction over transmission lines lower than 100 kV and the distribution system.

Exhibit 2 lists the existing Commission rules that touch upon the construction of new transmission and distribution facilities, recording interruptions and threats to the BES, capacity shortage emergencies, notification of electric utility outage events, and inspection of utility plant.

FPSC Rules for Transmission and Distribution Facilities	
Rules	**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 judgement of the utility.
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 2 *Source: Chapter 25-6, F.A.C.*

2.3.2 Commission Audit Staff 2014 Observations

In the 2014 report, audit staff included the following 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.

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

- 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 the Florida IOUs.

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

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

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

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

2.4 Florida Legislative Actions

A new 2017 Florida law (Section 330.41, Florida Statutes - Unmanned Aircraft Systems Act) prohibits a person from operating a drone over a critical infrastructure facility including an electrical power generation or transmission facility, substation, switching station, or electrical control center. The law protects critical infrastructure facilities by prohibiting any person from knowingly or willfully:

- Operating a drone over a critical infrastructure facility, unless the drone is in transit for commercial purposes and is in compliance with Federal Aviation Administration regulations;

- Allowing a drone to make contact with a critical infrastructure facility, including any person or object on the premises of or within the facility; and,

- Allowing a drone to come within a distance of a critical infrastructure facility that is close enough to interfere with the operations of or cause a disturbance to the facility.

Persons who violate Section 330.41, Florida Statutes, commit a misdemeanor of the second degree for their first offense, and a misdemeanor of the first degree for any subsequent violation. A companion law, Section 330.411, Florida Statutes (Prohibited possession or operation of unmanned aircraft) states that a person may not possess or operate an unmanned aircraft or unmanned aircraft system with an attached weapon, firearm, explosive, destructive device, or ammunition.

Although the above Florida Department of Transportation statutes were effective July 1, 2017, utilities are limited in what type of response to employ if a drone flies over a critical utility asset. Disabling a flying drone would violate Federal Aviation Administration regulations. At this time, it appears reporting the flyover to local law enforcement may be the only viable action for a utility concerned about damage to or surveillance of its substation or power-production facilities.

2.5 Government Agencies and Industry Associations

2.5.1 Government Agencies

At the federal level, responsibility for cybersecurity oversight and the establishment of industry standards is shared among several organizations. Presidential Policy Directive 41 signed in July 2016, designates three agencies with as lead federal agencies for cyber incident coordination in the United States. Each agency has been designated as the lead federal agencies charged with directing a specific line of effort to combat cybersecurity threats:

- **Department of Justice (DOJ)** - The FBI and the National Cyber Joint Task Force are designated as the leads for threat response activities in view of the fact that significant cyber events often involve the possibility of a nation-state actor or have some other national security nexus;

- **Department of Homeland Security (DHS)** - The National Cybersecurity and Communications Integration Center is designated as the lead agency for asset response activities. To accomplish this, DHS develops partnerships and shares information with the private sector owner/operators of the majority of the nation's critical infrastructure. DHS also shares information with state and local government and with international partners, as cybersecurity threat actors are not constrained by geographic boundaries; and,

- **Office of the Director of National Intelligence** - The Cyber Threat Intelligence Integration Center within the Office of the Director of National Intelligence is the lead federal agency for intelligence support and related activities, responsible to integrate analysis of threat trends and events, to build situational awareness, and support interagency efforts to develop options for degrading or mitigating potential threat capabilities.

Other federal agencies and national groups are also involved in safeguarding assets against cybersecurity threats:

- **Department of Energy (DOE)** - The 2020 goal of DOE's Office of Electricity Delivery and Energy Reliability is a national electric power grid infrastructure resilient to cyber threats, with energy delivery systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

- **American National Standards Institute (ANSI)** - This body launched a cybersecurity portal in 2015 with a database of public and private sector resources providing information on the contributions of the standardization community addressing cybersecurity issues. The portal features cyber-related resources, including government and private sector cybersecurity initiatives, ANSI standards packages on IT security, and information on ANSI's conformity assessment activities.

- **National Institute of Standards and Technology (NIST)** - The measurement and testing laboratory's cybersecurity program recognizes that interoperability, usability and privacy are critical components of national cybersecurity and helps develop standards and best practices addressing these areas of concern. NIST's cybersecurity programs enable the development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

2.5.2 Industry Associations

- **Edison Electric Institute (EEI)** - The Edison Electric Institute represents all U.S. investor-owned electric companies, providing public policy leadership, strategic business intelligence, and conferences and forums targeted specifically on cybersecurity. EEI actively partners with federal agencies, seeking ways to improve sector-wide resilience to thwart cyber and physical threats. EEI also cooperates with other agencies, federal intelligence, and law enforcement to strengthen cybersecurity capabilities.

- **Institute of Electrical and Electronics Engineers (IEEE)** - IEEE is the largest association of technical professions in the world, with members in over 160 countries. Its objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering, and allied disciplines. In 2014, IEEE launched a program called the *IEEE Cybersecurity Initiative*, focusing on cybersecurity protection, fortification of hardware and software, cyber education, and best practices.

- **Electric Power Research Institute (EPRI)** - EPRI is an independent, nonprofit organization representing members generating more than 90 percent of electric utility revenue in the U.S. In collaboration with the electricity sector, EPRI seeks to make generation, delivery, and use of electrical power safe, reliable, affordable, and environmentally responsible. Cyber/physical security and data privacy issues are an

organizational priority and focus. Recognizing the increasing dependence of electrical generation, transmission, and distribution on information technology and telecommunications infrastructure to ensure grid reliability, EPRI engages in research to design and implement countermeasures protecting the grid from cyber and physical security threats. An example of this research is the three-year EPRI study of electromagnetic pulse (EMP) energy capable of damaging or destroying grid electronic components or communications networks.

- **North American Transmission Forum (NATF)** - Members include investor-owned utilities among others operating on the principle that exchange of information is key to improving reliability of North American transmission systems. NATF leveraged members' expertise to document current capabilities and propose redundancies for critical capabilities, so that operators can monitor and control the BES if primary control center capabilities are lost.

3.0 Duke Energy Florida, LLC

Duke Energy Corporation (Duke Energy or the company) supplies energy to about 7.2 million U.S. electric retail customers in the Carolinas, Midwest, and Florida. Duke Energy Florida (DEF) has 166 transmission and 234 non-BES[1] substations and serves about 1.8 million Florida customers with approximately 8,800 MW of generating capacity.

3.1 Organization

As shown in **Exhibit 3,** Duke Energy created a hybrid NERC Oversight Compliance Model to provide both centralized and decentralized responsibility for maintaining focus on NERC compliance. This hybrid organization holds senior management accountable for overseeing and maintaining NERC compliance for all of Duke Energy's six regulated utilities. At the same time, operational employees are responsible for implementing the NERC reliability standards within their respective business units.

Improvement Review Board

An Improvement Review Board (IRB)/Senior Management Committee, headed by the operations officer, provides senior executive oversight of the effectiveness of the NERC requirements. The Board is comprised of executive vice presidents reporting to Duke Energy's CEO. Since creating the Board, Duke Energy reports significant improvements in areas such as accountability, personnel cybersecurity training, and change management practices.

Electric Reliability Executive Steering Committee

Reporting to the Improvement Review Board is an Electric Reliability Executive Steering Committee (ERESC) that directly oversees Duke Energy's compliance program. The Committee resolves resource constraints and directs any necessary corrective actions to the NERC CIP Working Sponsors. Members of the Committee represent the various business units of Duke Energy. The Electric Reliability Executive Steering Committee meets monthly to ensure all NERC compliance directives and associated processes and procedures are being executed and adhered to.

CIP Senior Manager

NERC requires that each utility designate a CIP Senior Manager to oversee CIP compliance. According to CIP-003, Requirement 3, "the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP reliability standards, CIP-002 through CIP-011." Duke Energy assigned its Senior Vice President and Chief Security Officer as the enterprise-wide CIP Senior Manager. Specific responsibilities include performing compliance oversight functions through annual validation planning, quality assurance activities, metrics tracking, and coordination across business units.

[1] 232 substations operate at 69 kV and are treated as transmission systems. Only two substations have no transmission-related equipment and are treated as distribution systems.

NERC CIP Working Sponsors

The NERC CIP Working Sponsors are comprised of directors and management from the compliance department within each business unit (Enterprise NERC CIP Compliance) as well as management from the operations of each business unit (CIP Program Management). The Working Sponsors collaborate to ensure the Electric Reliability Executive Steering Committee directives are being carried out.

Enterprise NERC CIP Compliance/CIP Program Management

Enterprise NERC CIP Compliance consists of the compliance and operational functions within each of the eight business units, respectively. As shown in **Exhibit 3** the eight business units are: Transmission, Fossil/Hydro (FHO), IT, Cybersecurity, Enterprise Protective Services (EPS), Renewables, Nuclear, and Administrative Services.

Duke Energy's CIP Program Management communicates new and revised standards in monthly working sponsor meetings and in quarterly CIP Look Ahead meetings. CIP Project Management ensures the Duke enterprise has deployed processes and procedures that are in compliance prior to the enforcement date and implements updated CIP policy. The business unit managers are tasked with maintaining day-to-day NERC CIP compliance. To do so, employees in each business unit are provided with essential procedures and templates designed to achieve compliance.

NERC CIP-014 falls under the responsibility of the Transmission and Enterprise Protective Services business units. These units are held accountable for physical security protection of transmission stations, transmission substations, and associated transmission primary control centers. Enterprise Protective Services operates an Enterprise Security Command Center that provides centralized monitoring of Duke Energy's facilities spread across its multi-state service territory. The Command Center operates 24 hours every day, and through the use of virtual and visual information can automatically analyze and correlate alerts across Duke Energy's service territory.

Duke Energy's Cybersecurity business unit is responsible for monitoring real-time cybersecurity threats. Within the Cybersecurity business unit is a Cybersecurity Operations Center that consists of analysts dedicated to preventing cybersecurity breaches including the implementation of firewalls and malware protections.

Independent Oversight

The CIP Senior Manager presents an update on performance and concerns regarding cyber and physical security and NERC CIP compliance to the Board of Directors/Audit Committee, at a minimum, on an annual basis.

Corporate Audit Services creates an annual risk-based audit plan with input from compliance and security leadership to perform cyber and physical security audits as well as compliance activities. The 2018 audit plan includes multiple audits ranging in focus from cybersecurity operations to internal penetration test processes to NERC CIP tools and procedures. After completing each audit, Corporate Audit Services publishes a detailed memorandum of findings and proposed management responses and actions to executive leadership. Resulting actions are assigned and tracked at the business unit level.

NERC Corporate Compliance currently serves as an independent oversight of NERC compliance. Members of NERC Corporate Compliance attend all NERC oversight meetings at the business unit and enterprise levels and provide input on compliance performance concerns and regulatory expectations.

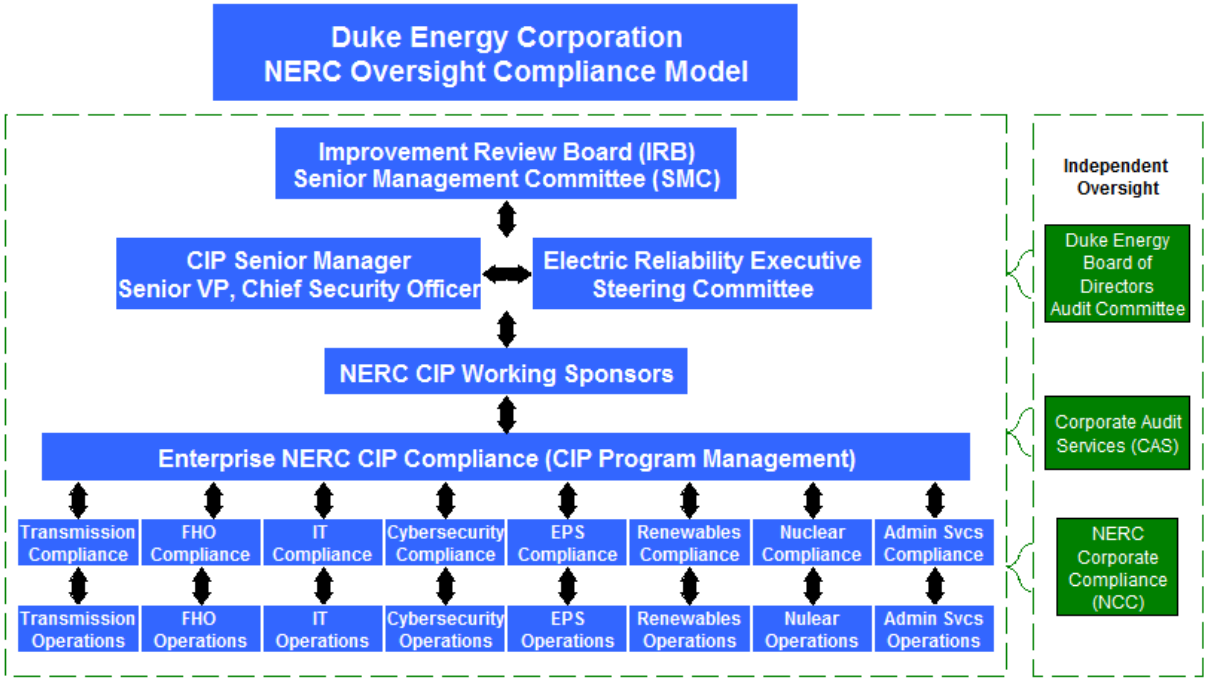


Exhibit 3 *Source: Document Request 2.1*

3.1.2 Cyber and Physical Security Policies and Procedures

Duke Energy developed and adopted an overarching IT 503 Program to oversee the implementation of NERC CIP reliability standards. The IT 503 Program is modeled after the NIST Cybersecurity Framework containing an array of activities, outcomes, and references which detail approaches to aspects of cybersecurity for both transmission and non-BES operations. The IT 503 Program addresses regulatory requirements and follows the five core functions of the NIST Framework: Identify, Protect, Detect, Respond, and Recover. Subsumed within the program are multiple IT cybersecurity standards that establish the requirements to comport with NERC reliability standards CIP-002 through CIP-011 and EOP-004. Duke Energy's Chief Security Officer are responsible for ensuring the continued development and implementation of the company's cybersecurity standards.

Duke Energy's physical security policies and procedures for non-BES facilities and policies and procedures for compliance with NERC CIP-014 and Transmission Planning (TPL) standards are not incorporated within Duke Energy's IT 503 Program. Instead, the physical security policies and procedures for non-BES facilities are established and deployed by Duke Energy's Transmission organization and compliance with CIP-014 and TPL is accomplished through implementation of policies and procedures deployed by Transmission and Enterprise Protective Services.

BES IT Cybersecurity Standards

Duke Energy developed the *IT 503 Standards and Enterprises Interpretations and Procedures* to establish compliance with CIP-002 through CIP-011. The IT 503 Standards include the specific controls, best practice references, and templates to support NERC CIP compliance and retention of evidence. The IT 503 Standards include controls for the following areas:

- Asset Identification and Classification
- Cybersecurity Management
- Personnel Security Awareness and Training
- Network Security and Remote Access Management
- Physical Security Management (protection of cyber assets)
- System Security
- Incident Management
- Continuity Recovery Planning
- Change and Vulnerability Management
- Information Protection
- Identity Access Management

BES Physical Security Policies and Procedures

Duke Energy uses the requirements within the NERC CIP standards to achieve compliance with CIP-014. NERC CIP-014 requires Duke Energy to perform an initial risk assessment to identify critical BES locations and to evaluate potential vulnerabilities and threats for each identified location. The standard further requires Duke Energy to develop and implement a physical security plan to protect the identified assets and to have the plan verified by an independent third party. Duke Energy states that it has complied with the NERC CIP-014 requirements.

As a BES operator, Duke Energy is required by the NERC EOP standards to report physical security events, protect its transmission systems from geomagnetic disturbances, ensure control center functionality, and maintain blackstart and system restoration plans. Blackstart is the process of using a generating unit to restore an electric power station or part of an electric grid to operation without relying on the electric power transmission network. Transmission Operators, such as Duke Energy, must ensure reliability is maintained during restoration with priority placed on restoring the interconnection. Duke Energy meets the requirements of EOP-004 through the implementation of steps provided in its IT 503 Standards and its Security Incident Reporting Procedure.

Duke Energy is also required by the NERC TPL standards to document its methodology, criteria, and processes in order to ensure transmission planning is performed consistently. Under NERC TPL standards, Duke Energy is charged with planning its system in a manner that avoids uncontrolled cascading outages beyond predetermined boundaries. TPL standards mandate that interconnection requirements for all facilities involved in the generation, transmission, and use of electricity be documented. According to Duke Energy, its transmission system is planned to achieve compliance with NERC TPL standards, including the development of geomagnetic disturbance models.

For both NERC EOP and TPL standards, Duke Energy employs its NERC Standard Assessment and Implementation Procedure to evaluate and implement revisions to the standards. The primary purpose of this procedure is to assist Duke Energy's subject matter experts to achieve compliance prior to effective enforcement date of the standard or requirements.

Non-BES IT Cybersecurity Standards

Duke Energy developed the *IT 502 Industrial Control Systems Minimum Cybersecurity Standard* to establish compliance for Industrial Control Systems (ICS). The IT 502 Standard provides requirements and expectations for specifying the security controls for organizations and information that support Duke Energy's ICS used within DEF's distribution control center and non-BES substations. Similar to the IT 503 Standard for the BES, the IT 502 Standard includes controls for the following areas:

- Inventory Security Awareness Training
- Physical Security (protection of cyber assets)
- Access Management
- Incident Response
- Electronic Security Perimeter
- Ensure Update Capability
- Removable Media Safe Handling
- Configuration and Change Management
- Secure Procurement
- Monitoring Electronic Access

Non-BES Physical Security Policies and Procedures

Duke Energy has implemented an Enterprise Protective Services Physical Security Program with standards based on a high/medium/low risk structure that applies to all Duke Energy non-nuclear facilities. Operational Security, which is an organization within Enterprise Protective Services, is responsible for managing and implementing the Physical Security Program. The program includes performing physical security surveys, determining facility compliance with standards, identifying vulnerabilities and developing mitigation strategies.

Duke Energy's Transmission organization is responsible for physical security of non-BES substations. Inspection and maintenance processes are followed in accordance with the transmission policies and procedures. Visual inspections and operational functions are performed on a defined schedule. Areas to be inspected include perimeter fences, substation structures, and electrical equipment. Information collected is used to schedule maintenance and repairs, and to ensure system reliability.

3.2 Cybersecurity Protections

3.2.1 Transmission

BES disruption could lead to far-reaching and devastating impacts. Facilities included in DEF's portion of the BES include 166 transmission substations, and both the primary and backup

transmission control centers. Version 5 of the NERC CIP Reliability Standards brought *all* BES Cyber Systems and assets within scope for at least some of the CIP requirements.

As noted in Chapter 2, Version 5 of the NERC CIP reliability standards requires Duke Energy, for the first time, to ensure that *all* BES Cyber Systems at each critical asset be in scope for at least some of the CIP requirements. In other words, CIP Version 5 expanded prior protections to some systems and assets that were not addressed in previous CIP versions.

Version 5 of NERC CIP-002 specifically required Duke Energy to identify and designate each critical asset as a High, Medium, or Low Impact BES Cyber System. Transmission primary control centers are specifically required to be classified as High Impact BES Cyber Systems, while other critical assets that meet specific impact rating criteria are to be classified as Medium or Low.

While cyber controls and protections were already defined for High and Medium BES Cyber Systems in Version 5 of the CIP standards, cyber protections for Low Impact BES Cyber Systems were not defined until CIP-003 Version 6 was issued on January 21, 2016. The new Low Impact requirements are required to be fully implemented by September 1, 2018. They address the following four subject matter areas:

- Cybersecurity awareness
- Physical security controls
- Electronic Access Controls
- Cybersecurity Incident Response

Duke Energy states that it has implemented the required cybersecurity controls and protections for all critical assets categorized as High or Medium BES Cyber Systems and is in the process of implementing the controls for Low Impact BES Cyber Systems.

It should be noted that Duke Energy, in some cases, has implemented supplementary safeguards for Low Impact BES Cyber Systems that are not specifically required by the CIP Reliability Standards. According to Duke Energy, it has conducted cybersecurity vulnerability assessments that support the broader application of safeguards to some applications even where not presently required by NERC.

Personnel and Training

CIP-004 requires personnel and training processes and procedures to minimize risk against compromise that could lead to misoperation or instability of the BES. The CIP-004 requirements include documented programs for:

- Personnel risk assessment
- Cybersecurity training
- Security awareness
- Access management
- Access revocation

Duke Energy states all employees submit to a personnel risk assessment (background check) that complies with CIP-004. The company states that it has implemented personnel and training requirements for High and Medium Impact BES Cyber Systems (e.g., training on physical and electronic access controls and handling of BES cyber system information and storage). Although not required by CIP-004, Duke Energy also implemented a training program applicable to Low Impact BES Cyber Systems.

Duke Energy also has implemented documented processes regarding security awareness, access management, and access revocation programs. Examples include reinforcing cybersecurity best practices through various employee communications, authorizing personnel to have unescorted access to a physical security perimeter, and canceling unescorted access privileges. As part of the September 1, 2018 implementation deadline for physical security controls applicable to Low Impact BES Cyber Systems, Duke Energy intends to require each business unit (including transmission) to create and implement processes and procedures for physical access authorization, provisioning, and revocation for transfers and terminations.

Electronic Access

Duke Energy implemented electronic security perimeter controls for CIP-005 High and Medium Impact BES Cyber Systems. The company documented processes and procedures and implemented protections such as: firewalls to restrict electronic access to the BES cyber systems within the electronic security perimeter; protocols for inbound and outbound access permissions; and methods to detect known or suspected malicious communications. Duke Energy is currently developing similar electronic access controls for Low Impact BES Cyber Systems to be implemented by the CIP-003 Version 6 due date of September 1, 2018.

System Security Management

Duke Energy's System Security Management program is governed by CIP-007 requiring documented processes for ports and services, security patch management, malicious code prevention, and security event monitoring. Duke Energy states that it implemented the documented processes and the required controls to satisfy CIP-007. Although not required by CIP-007, Duke Energy states that it is currently developing similar controls for Low Impact BES Cyber Systems.

Change Management and Vulnerability Assessments

Duke Energy's configuration Change Management and Vulnerability Assessments are managed through implementation of the CIP-010 requirements for High and Medium Impact BES Cyber Systems. The requirements for change management include developing baseline configurations and documenting changes for operating systems, open source applications, network accessible ports, and security patches applied. CIP-010 further requires Duke Energy to conduct and document vulnerability assessments for each BES cyber system. Duke Energy states that it maintains documented processes and has implemented the controls as they relate to CIP-010. Although not required by CIP-010, Duke Energy states that it is currently developing similar controls for Low Impact BES Cyber Systems.

Proposed NERC Standards

As previously mentioned, NERC is in the process of finalizing two new CIP reliability standards, CIP-012 and CIP-013. CIP-012 will require protections for communication network components

and data communicated between all transmission primary control centers in keeping with the risk posed to the BES. The standard is anticipated to become effective in mid-2018, with a 24-month implementation period.

CIP-013 will address security controls for supply chain risk management of BES cyber systems. Duke Energy has developed a supply chain risk management program using a number of resources which include the following:

- NIST Security/Privacy Controls for Federal Information Systems and Organizations
- NIST Guide for Conducting Risk Assessments
- Cybersecurity Procurement Language for Energy Delivery Systems

Duke Energy states that it has implemented controls to identify and assess cybersecurity risks to the BES from vendor products or services. These controls include protocols for risk assessment of vendors and specific contractual language to be used when a third party will have external access to Duke Energy's systems.

3.2.2 Non-BES

As previously mentioned, NERC CIP reliability standards are designed to protect the BES. These standards exclude the distribution system, including DEF's 234 non-BES substations that fall within the Commission's reliability jurisdiction. Since disabled distribution substation can be rerouted in quick order with limited customer impacts, distribution substations are not as valuable as targets of attacks for the purpose of system disruption.

Through Duke Energy's *IT 502 Industrial Control Systems Minimum Cyber Security Standard* for non-BES operations, the company has implemented numerous safeguards for cybersecurity protection. Many of the same procedures to protect transmission operations are in place regarding personnel and training, electronic security perimeters, system security management, vulnerability assessments, change management, incident reporting and recovery.

Examples of implemented protections for personnel and training include pre-employment background screening, and an access management program to oversee the authorization of user electronic access based on need. Other implemented protections for electronic security and system security management include electronic access points, intrusion detection, remote access management, patch management, antivirus software, and change control and testing.

Additionally, the company is in the process of integrating information and operational system technologies and will work towards mitigating any associated vulnerabilities.

3.3 Physical Security Protections

3.3.1 Transmission Facility Protections

Pursuant to NERC CIP-006, Duke Energy is required to have documented physical security plans for the protection of High and Medium Impact BES Cyber Systems associated with each asset. These include facilities such as primary and backup control centers, transmission stations

and substations, and substation control houses. At a minimum, the required CIP-006 physical security plans and programs must address perimeter protection of cyber assets, physical assets, physical access points, protection of control systems, protection of electronic access control systems, and procedural controls for monitoring physical access. Examples of protections include lists of authorized individuals, access logs, alarm systems, motion sensors, electronic readings, and secured cabling.

According to Duke Energy, it has implemented all required physical security protections to comply with CIP-006. The NERC standard for CIP-006 requires locally mounted hardware or devices at the security perimeter such as motion sensors, electronic lock control systems, and badge reader. The company is developing physical security controls for Low Impact BES Cyber Systems to be implemented pursuant to CIP-003 Version 6 by September 1, 2018.

In response to the Pacific Gas and Electric Metcalf substation attack in 2013, NERC moved quickly to create CIP-014. The purpose of CIP-014 is to identify and protect all critical BES facilities such as primary control centers, transmission stations, and substations whose loss could result in widespread outages if rendered inoperable. At a basic level, the standard requires additional layers of physical security for the surrounding property borders.

The standard requires the implementation of physical controls to protect the reliability of the BES, but allows the utility to determine appropriate protective equipment to be deployed. A best practice guide published by the North American Transmission Forum,[2] includes the following examples of protective equipment: perimeter signage, fencing, walls, locked gates, lighting, intrusion detection systems, vehicle barriers, alarms, video surveillance, and on-site security officers.

NERC CIP-014 requires Duke to develop and implement a documented physical security plan that covers transmission primary control centers and Medium Impact transmission facilities including stations and substations that meet the requirements of R1. In 2015, Duke identified its critical facilities to be covered in the security plan and performed threat and vulnerability assessments at each of these sites. The threat assessment team was comprised of members from Duke Energy's Enterprise Protective Services group, the Department of Homeland Security, and a third-party consulting firm.

Upon completion of the site assessments, Duke Energy retained the same third party to design and prepare engineering documents and drawings for construction of the security systems and physical security plan designated for each site. Duke Energy retained another third party to review its threat and vulnerability evaluations and security plans. This third-party reviewer confirmed Duke Energy met the CIP-014 requirements for each site with minor suggested wording changes to the security plan. Site preparation and construction began in the second quarter of 2016 and the plan for each identified site was completed in early 2017. For new construction, such as transmission substations and associated primary control centers, DEF establishes its implementation schedule and NERC verifies that the company is on schedule.

[2] North American Transmission Forum Practices Document for NERC Reliability Standard CIP-014-2 Requirement R5, 2017.

Aside from the CIP Reliability Standards, Duke Energy employs its own physical security program to perform risk and vulnerability assessments identifying additional security measures needed. For example, the company is in the process of designing and implementing additional physical security controls for facilities outside the scope of CIP-014. Duke Energy also performs monthly inspections on all transmission substations.

Since 2014, Duke Energy has implemented changes to its physical security protection protocols, including the hardening of its control centers to better detect, delay, and deter physical attacks. A Transmission Substation Security Team was also established in 2015 to focus on issues associated with the installation of new security equipment for transmission facilities (i.e., equipment ownership, ongoing maintenance, emergency repairs, compliance and operational protocols).

3.3.2 Non-BES Facility Protections

Although minor intrusions, thefts, and acts of vandalism on distribution facilities do occur, none is likely to cause outages affecting the stability of the grid. By the nature of system design, a distribution substation outage will have only limited impact. However, physical security for distribution facilities is a significant concern. Potential results of a successful physical attack on distribution facilities can include death or injury to the public or workers, and costs of equipment replacement.

While CIP standards are limited to the BES, Duke Energy states it is currently in the process of improving its non-BES grid protections to make the system more secure and resilient, decrease outages, and enable faster restoration. Examples of protections currently in place include restricting, monitoring, and alarming physical access. Duke Energy's existing policies and oversight activities for its non-BES inspection and maintenance program are the responsibility of the Transmission organization.

Inspections are performed on all non-BES substations, and Duke Energy's Enterprise Protective Services unit conducts assessments and consults with distribution operations to implement a security profile for non-BES locations. The assessments include physical security elements. New digital devices and communications and control systems ("smart grid" devices) are also being deployed at the non-BES level to increase physical plant security as well as cybersecurity.

3.4 Collaborative Resources

3.4.1 Industry Groups and Government Agencies

Duke Energy works closely with numerous industry groups and government agencies to enhance cyber and physical security protections and allow for timely response to any future security breach event. Some specific collaborative entities include:

North American Transmission Forum (NATF)

Duke participates in the NATF Physical Security Working Group which meets monthly and gathers security professionals within the electric utility industry. NATF promotes information exchange regarding industry trends, best practices, and promotion of peer review of security-

related activities. NATF additionally provides a platform for members to submit surveys that gather information on benchmarking, security practices, and lessons learned.

EEI / American Gas Association (AGA) Physical Security Group

Edison Electric Institute (EEI) and AGA are the industry associations for U.S. investor-owned electric companies and energy companies that deliver natural gas. Duke Energy interacts with EEI and AGA on numerous technical, research, and regulatory matters involving cyber and physical security issues. The joint working group provides high-level industry incident awareness and a forum to discuss and recommend industry best practices. Duke Energy also participates in EEI's Spare Transformer Equipment Program (STEP) to create 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.

Electric Power Research Institute (EPRI)

Duke Energy works closely with EPRI, as a member, in various capacities regarding cyber and physical security research projects. One project involves a three-year impact study addressing potential combined electromagnetic pulse (EMP) effects on the BES. The study focuses on the following prioritized actions associated with:

- Overheating of transformers caused by geomagnetic-induced currents (E3 pulse)
- Overvoltage situations caused by lightning-strike equivalents (E2 pulse)
- Damage to electronics and control systems caused by high-amplitude pulses with short durations (E1 pulse)

The results of this study should provide Duke Energy with technical knowledge needed to guide future investment to protect its critical infrastructure facilities against EMP effects.

Local, State, and Federal Law Enforcement

Duke Energy collaborates with local and federal law enforcement entities to maintain awareness of potential security threats. These include local police, Coast Guard, and the Federal Bureau of Investigation (FBI). The company also partners with FBI/Infragard, a non-profit organization providing public-private collaboration to exchange information and promotes mutual learning opportunities relevant to the protection of critical infrastructure.

Department of Homeland Security (DHS)

DHS's flagship program is the Cyber Information Sharing and Collaboration Program (CISCP). CISCP is a public-private program which complements ongoing DHS information sharing of information regarding cyber threats, incidents, and vulnerabilities among energy sector partners. Duke Energy participates in fusion centers that were created by DHS for the purpose of accessing highly sensitive shared information and intelligence. The shared information provides Duke Energy with a higher level of awareness and preparedness for any identified threats.

NERC CIP Committee (CIPC)

CIPC is a NERC Committee that coordinates NERC's security initiatives and serves as an expert advisory panel to the NERC Board of Trustees, standing committees in the areas of cyber and physical security, and the Electricity Information and Analysis Center (E-ISAC). CIPC educates the electricity subsector to maintain critical infrastructure security.

Department of Energy (DOE)

CRISP is a public-private partnership managed by E-ISAC and cofounded by DOE, NERC, and industry partners. Duke Energy has been voluntarily participating in CRISP since 2014. CRISP is focused on developing situational awareness tools that enable the energy sector to better protect critical infrastructure and key resources through the exchange of detailed cybersecurity information. Participation in CRISP allows utilities to share real-time threat information anonymously and to identify additional safeguards as needed. CRISP also provides access to advanced threat and FBI intelligence information regarding DEF's own network.

3.4.2 Exercises and Assessments

Duke Energy is required to comply with NERC reliability standards but must also focus on self-assessments and internally-initiated actions to manage cyber and physical security risks. Duke Energy employs a standard risk management framework, including use of a risk matrix, to manage ongoing and emerging risks. This framework includes the following process components: risk identification, risk evaluation and assessment, mitigation response, reporting, and monitoring.

Duke Energy also participates in drills and voluntary programs in coordination with federal, state, or local emergency authorities. Drills range from malware detection, tabletop exercises to activating command and control structures.

GridEx IV

GridEx is a biennial North American grid security and emergency response and recovery exercise run by NERC. Through GridEx, industry, law enforcement, and government agencies participate collaboratively to simulate cyber attack conditions and responses. On behalf of Duke Energy Corporation, Duke Energy-Carolinas' and DEF's Transmission System Operations Center actively participated in the most recent GridEx IV exercise in November 2017. Duke Energy senior management believes the company continues to benefit from lessons learned from GridEx IV. Following GridEx IV, Duke Energy plans to further refine its incident response, recovery plans, information sharing, and coordination to better respond and recover from potential attacks.

Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model (C2M2) was developed jointly by the Department of Energy, Department of Homeland and Security, and industry partners. C2M2 is a self-evaluation tool used to measure the maturity of its cybersecurity control capabilities to address vulnerabilities. In the summer of 2015, Duke Energy established and completed the steps necessary to identify needs and priorities for cybersecurity improvements resulting from the C2M2 program.

Event Analysis Process (EAP)

NERC's EAP is a collaborative effort between NERC and the eight Regional Entities to provide information on the categories and causes of reportable events, including potential threats or vulnerabilities to BES reliability. Lessons learned through participation in EAP can help utilities identify needed changes to operating procedures, personnel training, or identify equipment problems, such as loss of supervisory control and data acquisition (SCADA) operating and monitoring ability. Duke Energy participates in the EAP.

Enhanced Cybersecurity Services (ECS) Program

ECS is a Department and Homeland Security intrusion prevention program that Duke Energy participates in to protect computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with three accredited Commercial Service Providers: AT&T, CenturyLink, and Verizon. These providers use the information to block certain types of malicious traffic from entering customer networks. ECS is meant to augment, but not replace, existing cybersecurity capabilities.

US-CERT / ICS-CERT Computer and Cyber Readiness and Response Teams

DHS also developed the U.S. Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) public-private partnership. US-CERT and ICS-CERT are responsible for analyzing and reducing cyber threats and vulnerabilities, coordinating incident response activities, and strengthening the security of industrial control systems through a comprehensive cybersecurity program. Through ongoing alerts from ICS-CERT, Duke Energy applies the threat intelligence to its cybersecurity controls to protect its critical infrastructure assets.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a US Government policy guidance that provides basic processes and essential controls for organizations to understand, manage, and reduce cybersecurity risks through the five core functions: identify, detect, protect, respond, and recover. Duke Energy uses the NIST Framework to develop effective cybersecurity strategies tailored to its particular combinations of smart grid-related characteristics, risks, and vulnerabilities.

3.4.3 Audits

NERC Rule of Procedure 403.11.1 states that for an entity registered as a Balancing Authority, Reliability Coordinator, or Transmission Operator, a compliance audit will be performed at least once every three years. The compliance audit involves a systematic, objective review and examination of records and activities to determine whether Duke Energy is in compliance with applicable reliability standards such as CIP, EOP, and TPL.

Southeastern Electric Reliability Corporation (SERC), the Florida Regional Coordinating Council (FRCC) and ReliabilityFirst Corporation have conducted audits of Duke Energy's compliance with the NERC reliability standards. The audits consisted of site assessments, review of programmatic documentation and evidence, and on-site interviews of subject matter experts. Duke Energy responded to any deficiencies identified by NERC and corrective actions taken are documented to ensure compliance.

Duke Energy also internally self-reports potential non-compliance issues to NERC Corporate Compliance. The company uses an issue management process for identifying and reporting possible violations. The self-reported information needs to be of type and quality necessary for SERC to render an informed final decision on the system risk posed by the possible violations. According to Duke Energy, it follows the self-reporting procedures prescribed by NERC. Duke uses an enterprise NERC compliance tracking tool to document compliance, record potential violations, including self reports and mitigation plans. Compliance metrics are pulled from this tool and provided to the Electric Reliability Executive Steering Committee.

Upon final review of all potential self-reported non-compliance issues, the Regional Entity informs Duke Energy of a mitigation plan, if necessary, to resolve any resulting audit findings or open enforcement action items still pending. Duke Energy establishes a mitigation schedule which is not to extend over one year and milestones are to be filed within 90 days as required.

3.5 Incident Reporting, Response, and Recovery

3.5.1 Reporting and Response Planning

NERC CIP-008 and EOP-004, respectively, specify cyber and physical incident reporting and response planning requirements that apply to High and Medium, as well as Low Impact BES Cyber Systems pursuant to CIP-003 Version 6. According to Duke Energy, it is in compliance with all of the NERC and DOE incident reporting and response planning requirements. To further improve upon its cyber and physical security incident reporting and response processes and procedures, the company also states that it interacts with the following entities:

North American Electric Reliability Corporation (NERC)

NERC's role in responding to a blackout or other major BES disturbance is to provide leadership, coordination, technical expertise, and coordinate assistance among industry stakeholders and government agencies. The Electricity Information Sharing and Analysis Center (E-ISAC) within NERC receives and analyzes cyber and physical security incident reporting data via a secure portal and coordinates incident management and communicates mitigation strategies with the electric industry and government partners. E-ISAC also manages the Cybersecurity Risk Information Sharing Program (CRISP) to facilitate timely exchange of detailed cybersecurity information among energy sector partners so they can better protect critical infrastructure and key resources.

Department of Energy (DOE)

The DOE has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States via Form OE-417. Analysis of the data may be used for DOE investigations of BES reliability issues resulting from cyber and physical security incidents.

According to Duke Energy, the conditions requiring the filing of Form OE-417 to DOE would also likely trigger reporting to the Commission per FPSC Rule 25-6.018, F.A.C. Since 2014, DEF has not experienced any reportable cyber or physical security incidents.

Florida Department of Emergency Management (FDEM)

Duke Energy states that its incident response and crisis management activities are dictated by the necessary response level and nature of the event. For cyber or physical security incidents that have the potential to significantly impact Duke Energy, procedures within Duke Energy's Enterprise Emergency Management Program require notification to the FDEM and the Florida Homeland Security.

Florida Public Service Commission

In the event of a cyber or physical security emergency incident, Duke Energy states that "a call by DEF to the Division of Emergency Management is a communication with the FPSC." The Commission serves as the primary agency for the Emergency Support Function (ESF-12) for energy-related emergencies and DEF works closely with FDEM until service is restored. Therefore, the company expects the information flow will adequately keep the Commission informed. Duke Energy further noted that other means of communication are available for informal notification in the event of a significant outage caused by a cyber or physical attack. For example, when Duke Energy learned in late 2017 of a possible security breach at one of its payment processors, TIO Networks, DEF representatives contacted the FPSC to provide an update.

Local, State, and *Federal Law Enforcement*

Within Duke Energy, the IT Security organization maintains points of contact with the FBI Cyber Task Force at the Charlotte Field Office. Duke Energy would work with the Florida Department of Law Enforcement (FDLE) in a cybersecurity incident if the incident were precipitated by suspected criminal activity. FDLE would then activate its Cyber High Tech Unit, and the Florida Computer Crime Center would be the point of contact.

3.5.2 Recovery Planning

Recovery and restoration planning requirements are contained in the NERC reliability standards such as CIP-009, EOP-005, EOP-008, and EOP-011.

For CIP-009, the recovery plans for High and Medium Impact BES Cyber Systems include: specifications for activation; procedures for responders; processes for backup and storage of information; implementation and testing; and recovery plan review, update and communication. According to Duke Energy, it has met the requirements of this standard.

Duke Energy states that it has implemented the restoration plans required by EOP-005 addressing detailed strategies and priorities for restoration. They address the following: coordination with the reliability coordinator on high-level strategy for restoration; description of how prioritized off-site power to nuclear power plants will be fulfilled; procedures for restoring interconnections with other transmission operators; and processes to restore loads for system restoration such as station service for substations.

Specific to EOP-008, the requirements focus on maintaining reliable operations of the BES in the event that primary control center functionality is lost. Duke Energy has implemented the requirements to comply with EOP-008 including: a documented plan containing, at a minimum, location and method of implementing backup functionality; description of supporting elements

such as tools and applications for situational awareness, data and voice communications, cyber and physical security, and power sources.

Pursuant to EOP-011, Duke Energy is required to develop, maintain, and implement operating plans that includes processes and procedures to prepare for and mitigate emergency situations. Duke Energy states that it is in compliance with the above EOP standards.

These EOP and CIP standards also require DEF to conduct and document incident response and restoration plan reviews and tests at least annually. According to Duke Energy, the lessons learned through reviewing, testing, as well as participating in the Spare Transformer Equipment Program (STEP) and operational exercises, such as GridEx, should allow for more effective incident response and recovery.

3.6 Cyber and Physical Security Cost Tracking

Duke notes the broad categories of projects included in DEF's transmission and distribution capital budget make it difficult to identify and isolate spending and investment specifically for cyber and physical security activities. Since 2016, Duke Energy has staffed an independent Project Management organization dedicated to security initiatives. All of these costs are tracked with their respective cost centers. Duke Energy's business units can track physical security costs within their respective capital and operating budgets; however, no methods exist to track these costs across business units. Examples of physical security costs include cameras, fencing, and card access readers. These costs are included in capital projects or imbedded in other expense categories under operations and maintenance budgets.

4.0 Florida Power & Light Company

Florida Power & Light Company (FPL) serves nearly five million customers across the state of Florida with approximately 26,000 MW of generating capacity. FPL is a subsidiary of NextEra Energy, Inc. (NextEra Energy) and is registered with the Florida Reliability Coordinating Council (FRCC) as a Transmission Owner, Operator, Planner and Service Provider, Balancing Authority, Distribution Provider, Planning Authority, and Resource Planner. FPL owns 110 transmission substations and 500 distribution substations within its service territory.

4.1 Organization

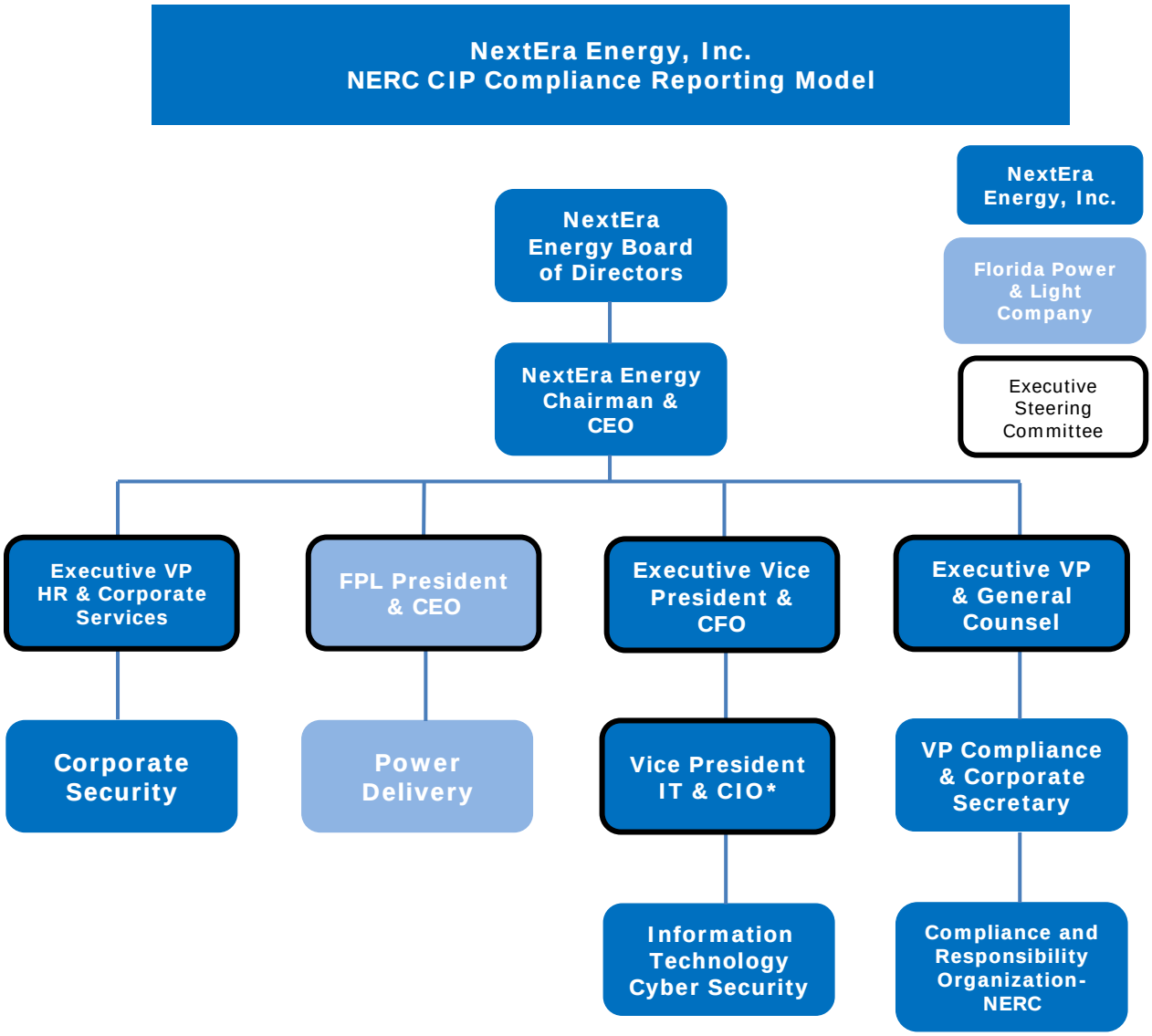
4.1.1 Compliance and Responsibility Organization

Florida Power & Light splits the responsibility of NERC CIP standard compliance among several organizations throughout the company. The NextEra Energy Compliance and Responsibility Organization-NERC (CRO-NERC) specifically deals with NERC standards compliance. The Compliance and Responsibility Organization reports to the Vice President of Compliance as shown in **Exhibit 4**. The CRO-NERC organization works collaboratively with individual business units such as Power Delivery, Information Technology (IT), and Corporate Security to monitor the overall compliance with NERC CIP standards. These FPL business units are responsible for implementing and maintaining the day-to-day compliance with NERC CIP standards.

The CRO-NERC organization, in coordination with the Federal Regulatory Affairs group, advises FPL's business units on new or revised compliance deadlines. The CRO-NERC organization developed the *NERC Internal Compliance Plan*, which lays out the roles, responsibilities, and processes for compliance of all NERC standards. These include:

- Document management and record retention
- Training
- Internal assessments
- Spot-checks and self-reporting

The compliance plan applies to all NextEra Energy assets and facilities. FPL's business units rely on embedded management controls to monitor compliance activities required by NERC. For example, business unit management conducts random sampling of logs and procedures. Besides the business unit management controls, the CRO-NERC organization monitors NERC compliance by conducting internal assessments, reviewing business units' compliance documentation, and interviewing FPL subject matter experts. NERC standards compliance status is reported by the CRO-NERC organization to senior management monthly. The business units also conduct self-assessments of each NERC standard and requirement when needed. Most recently, these assessments were performed during the transition from CIP Version 3 to Version 5.



*CIP Senior Manager

Exhibit 4

Source: Supplemental Email

4.1.2 CIP Senior Manager – Vice President and CIO

NERC requires that each utility designate a CIP Senior Manager to oversee CIP compliance. According to CIP-003, Requirement 3, "the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011." For NextEra Energy, the designated CIP Senior Manager is the Vice President and Chief Information Officer as shown in **Exhibit 4**. The CIP Senior Manager delegates the responsibility and authority for NERC CIP compliance to the CRO-NERC organization, the Cyber security organization, and Corporate Security.

4.1.3 Information Technology Cyber Security Organization Department

NextEra Energy IT Cyber security department shares responsibility for cybersecurity standards CIP-002 through CIP-011. The Cyber security department is also responsible for the cyber

security of all NextEra Energy systems. This business unit monitors, detects, and responds to cyber security threats. The Cyber security department reports directly to NextEra's designated CIP Senior Manager as shown in **Exhibit 4**.

FPL has developed a Cybersecurity Governance model that requires the Cyber security department to report to upper management on a regular basis. Monthly meetings are held with the Cyber security and IT risk working group, which develops and monitors the strategic plan and emerging risks. The Cyber security organization reports quarterly to the Cybersecurity Executive Steering Committee, which is comprised of the Vice Presidents of multiple business units, including Finance, Power Delivery, Business Management, IT, and General Counsel. They manage the enterprise cyber risks, approve the strategic plans, and track the programs performance and progress. Annually, the Cyber security department reports to the Board of Directors who ensure that the company is appropriately addressing risk throughout the whole enterprise.

Additionally, the Cyber security department assesses the company's technology risk management processes and reports quarterly to FPL's Risk Management function. An on-call IT Cyber security Analyst with the Cyber security department receives any alerts of cyber threats during off hours. FPL is in the process of creating a Cybersecurity Operations Center, which will be manned 24/7.

FPL has also made significant investments to enhance cybersecurity throughout all NextEra systems. This includes increasing Cyber security department staffing as well as investing in new technology and controls such as a new anti-virus system, revamping the cyber access management process, and acquiring new incident detection and response technology.

4.1.4 Corporate Security Department

FPL's Corporate Security department is responsible for the security management of all non-nuclear NextEra Energy facilities. These responsibilities include identifying and managing all security risks, providing incident response, and overseeing the physical security of all FPL facilities.

Corporate Security has divided FPL's service territory geographically into five regions each staffed by an Area Security Manager. Centrally, one Security Operations Center monitors all FPL access control, intrusion detection, and video surveillance systems. The Center is manned 24 hours by 10 full-time employees working rotating shifts. The Center serves as a point of contact for local law enforcement and employees to report concerns about the security or answer any questions pertaining to FPL's facilities. The Center is authorized to utilize the company's mass notification system for employees in case of an emergency.

Corporate Security contracts with a third-party contractor who collects and analyzes data collected from the web through key word searches. The contractor provides Corporate Security with daily reports, which are reviewed to determine any action needed.

FPL's Corporate Security also receives security information from government and industry peer groups including the FBI, Department of Homeland Security, and Fusion Centers. An in-house

intelligence analyst monitors information coming from these groups to identify trends or emerging threats to NextEra Energy facilities. Corporate Security also participates in monthly conference calls offered by groups such as E-ISAC that discuss security threats and best practices.

4.1.5 Cyber and Physical Security Policies and Procedures

NERC Cyber Security Policies

FPL has implemented a corporate level *NERC Cyber Security Policy* to ensure adherence to the NERC CIP standards. This document defines the CIP requirements applicable to High, Medium, and Low impact BES cyber systems. This plan is owned and maintained by the IT Cyber Security department. All applicable business unit compliance managers as well as the NERC CIP Senior Manager are required to review the policy once a year.

NERC Physical Security Policies

FPL has also drafted and implemented the *Enterprise Physical Security Plan CIP 006-6*. This plan defines the programs, standards, and procedures that provide physical security protections for the identified BES cyber assets and systems in all of NextEra Energy's facilities in accordance to the NERC CIP standards. This document is to be reviewed annually by FPL personnel to ensure compliance with requirements for affected critical facilities.

Additionally, the *Enterprise Physical Security Plan CIP-014-2* defines NEE enterprise Physical Security Plan and related program, which will provide physical security protections for identified transmission stations, transmission substations, and primary control center to comply with CIP-014. This plan was developed reviewing the Facility Security Reviews of substations and control centers identified under CIP-014.

FPL implemented the *Geomagnetic Disturbance Operations Procedure* as required by EOP-010. This procedure outlines the necessary actions the company would take in order to respond to a Geomagnetic Disturbance event.

Distribution Policies

FPL has implemented the *Cyber Access Policy* for all corporate cyber assets including the company's distribution cyber assets. This policy establishes the requirements for the request, monitoring, usage, and termination of electronic access to the company's cyber resources. FPL uses the National Electric Safety Code Section 11 requirements as guidance for its distribution substation physical security design.

4.2 Cybersecurity Protections

4.2.1 Transmission

As noted previously, NERC CIP standards focus on the Bulk Electric System. FPL's BES cyber systems and assets are housed in facilities such as generating sites, transmission control centers, and ~110 transmission substations.

As stated in Chapter 2, Version 5 required all companies to ensure all BES Cyber Systems and assets expanding the list of systems and assets protected under previous NERC CIP versions. FPL states that it is currently in compliance with Version 5 of the NERC CIP Reliability Standards. During the transition from CIP Version 3 to Version 5, FPL's CRO-NERC organization created an enterprise-wide process to classify all NextEra Energy assets in accordance to NERC CIP-002. This process was used to identify and classify those assets in a consistent way by all impacted FPL business units that owned BES cyber assets. These assets are classified as High, Medium, and Low Impact. Currently, most NERC CIP Reliability Standards apply to only High and Medium Impact systems and assets.

FPL states that as of April 1, 2017 it had updated relevant cyber security policies, standards, and procedures for Low Impact BES cyber assets. The company is implementing additional cyber security measures for Low Impact cyber assets that are due to be completed by September 1, 2018.

Personnel and Training

FPL has implemented various personnel and training requirements to meet NERC CIP-004 for its High and Medium Impact BES cyber facilities and systems. The company developed a corporate Security Awareness Program, to ensure all personnel working with BES cyber assets and systems maintain awareness of physical and cyber security best practices. Additionally, FPL has created an enterprise-wide NERC CIP training model for both employees and contractors with NERC CIP compliance responsibilities. This training is required before access is granted to BES cyber assets. FPL conducts Personnel Risk Assessments of all employees and contractors needing access to BES cyber assets. The company manages all CIP cyber asset access through a centralized enterprise-wide access management system. The company uses this central system to manage role-based access control and the verification processes to approve access to BES cyber assets. Although not currently required by NERC CIP-004, FPL employs the same Security Awareness Program for Low Impact BES Cyber Systems as for High and Medium Impact.

Electronic Access

As required by NERC CIP-005, all High and Medium Impact BES cyber systems and their assets are located within an electronic security perimeter. The company restricts access to the electronic security perimeter through the use of firewalls as the electronic access point. High Impact BES cyber systems use a unique class of firewalls providing different protection than those used for Medium Impact cyber systems. FPL also uses Intrusion Detection Systems and Intrusion Protection Systems at electronic access points. While there is currently no existing NERC CIP-005 requirement for Low Impact BES Cyber Systems, the company is currently assessing the implementation of similar processes for these systems. Currently, Low Impact BES Cyber Systems are protected by firewalls and routers with access control lists.

System Security Management

Various FPL policies also apply to all NextEra Energy cyber systems. These policies provide a framework for security controls for all corporate systems. Though not required by NERC CIP-007, FPL uses the *Cyber Access Policy* for all NextEra Energy cyber assets. This policy covers the internal controls and procedures to grant, limit, and revoke electronic access to all NextEra Energy cyber systems. All employees and contractors that require access to the NextEra Energy network take the Information Security Awareness training. The company restricts employee and

contractor network access to management-approved purposes using the principle of Least Privilege. FPL revokes access to the network when an employee or contractor is terminated or when system access is no longer needed.

Change Management and Vulnerability Assessment

As required for NERC CIP-010, FPL has implemented the *Configuration Change Management Procedure*, which details the procedure to approve and document changes to the configuration baselines of High and Medium Impact BES Cyber Systems. All changes must be tested before implementation to the BES cyber systems. As required for NERC CIP-010, the company performs annual vulnerability assessments that cover network discovery, network ports and services identification, physical walk-down of BES Cyber Assets, and wireless review. Although not required by NERC CIP-010, Low Impact BES Cyber Systems are managed by the corporate Change Management Policy and established FPL practices. The protective relay settings for Low Impact BES Cyber Systems are also stored in a database where field engineers can check to see if they are being appropriately implemented.

Proposed NERC Standards

The CRO-NERC organization is currently monitoring the development of CIP-012 and CIP-013, which are still under development explained in Chapter 2. CIP-012 will require protections for communication network components and data communicated between all transmission primary control centers according to risk posed to the BES. The standard is anticipated to become effective June 2018.

CIP-013 will address security controls for supply chain risk management of BES cyber systems. This will against vendor control weaknesses compromising FPL's cyber assets and systems. Currently, the IT Cyber security department has implemented periodic internal cyber security assessments to review potential security risks that suppliers might pose through the supply chain process. The Cyber security department also works with the application development teams to test the security of the applications used in the NextEra Energy networks.

4.2.2 Distribution

FPL's distribution control centers and ~500 distribution substations fall within Commission reliability oversight jurisdiction and have minimal association with the NERC CIP Reliability Standards. However, in many cases, customers served from a distribution substation that has lost functionality can be restored through rerouting or other means in quick order with customer impacts avoided or limited. Thus, distribution substations are not considered valuable targets if the purpose of the attack is to disrupt the system.

FPL's Distribution Control Centers house distribution cyber system applications and assets. To protect these assets, the company employs the same Security Awareness Program, training, and access management system as for BES cyber systems. Various personnel and training policies that apply to NextEra Energy cyber systems also apply to distribution cyber systems. Since the distribution cyber systems utilize High Impact BES Cyber Assets to run applications such as SCADA, they are afforded the same electronic security perimeter protections. The distribution cyber system, not located within High Impact BES Cyber Assets, are located within secure networks.

FPL performs monthly patch management activities on distribution control and monitoring application running on the control center infrastructure. All distribution cyber assets are governed by the *Cyber Access Policy*. Similar to Low Impact BES Assets, distribution cyber systems are managed by the corporate Change Management Policy and established FPL practices. The protective relay settings for Low Impact BES Cyber Systems are stored in a database where field engineers can verify whether they are being appropriately implemented.

While the distribution system is not subject to all NERC CIP Reliability Standards, FPL still uses the standard security design for all distribution and transmission substations. This includes substation protective relays, password protection for substation communication processors, and locked relay vault doors. Distribution cyber assets located within substations are electronically protected by firewalls and routers with access control lists.

4.3 Physical Security Protections

4.3.1 Transmission Facility Protections

NERC CIP-002 requires FPL to classify all of its BES Cyber Systems, including its control centers and transmission substation operating at 100 kV or above, as High, Medium, or Low Impact.

NERC CIP-006 requires implementation of physical security plans and procedures to monitor the access and protections of the physical perimeter of the BES cyber assets. These assets include primary and backup control centers and some transmission substation control houses. Specific plans are mentioned in more detail in Subsection 4.1.5.

All Medium and Low Impact FPL substations are equipped, at a minimum, with the standard enterprise-wide substation security measures, which include chain-link fences, concrete vault with steel doors to protect the relays, lighting, and locks at the perimeter gate and vault entrances. As required by NERC CIP-006, High and Medium Impact facilities have varying levels of badge access readers, intrusion detections analytics, and cameras.

While not required by NERC CIP-006, FPL has voluntarily implemented a defense-in-depth approach using physical security measures such as a badge reader and lock/key combination for Low Impact substations. While transmission substations operating below 100 kV fall outside of the NERC CIP Reliability Standards, FPL still uses the standard security protection design specifications including chain-link fences, concrete block vault with steel doors to house the relays, lighting, locks at the perimeter gate and vault entrances.

As required by NERC CIP-006, FPL manages and assesses the physical security of facilities containing High and Medium Impact BES Cyber Systems through Facility Security Reviews. FPL's Area Security Managers are to conduct Facility Security Reviews every two years. These provide an assessment of the facility's physical security measures. Facilities rated as Low Impact are not required to receive Facility Security Reviews.

However, while not required by NERC CIP-006, all transmission substations are inspected by the Facilities Management contractor who performs quarterly Substation Assessments. These assessments review the physical security measures and the condition of the substation equipment. The assessments are reviewed by the Area Security Manager. FPL's Power Delivery business unit also conducts additional yearly substation condition assessments on all transmission and distribution substations.

As required by NERC CIP-006, FPL uses the Physical Access Control System to monitor access to the physical location of the BES cyber system. The Physical Access Control System is designed to send alerts if any intrusions occur.

CIP-014 focuses on the High Impact transmission primary control center and backup centers as well as specific Medium Impact BES substations that, if lost, could potentially cause a cascading outage throughout the FPL service territory.

As required by CIP-014, FPL conducted an analysis to identify the applicable facilities and develop a site-by-site vulnerability assessment and plan. The specific plan is discussed in more detail in Subsection 4.1.5. As required by CIP-014, FPL contracted with an unaffiliated third-party reviewer to verify FPL's risk assessment methodology used for CIP-014 facility identification, the analysis of the potential cascading effects involving these facilities, and the final list of identified facilities. A separate third-party security contractor reviewed the physical security plan for each CIP-014 sites.

The implementation of CIP-014 measures for these sites began in 2016 and is expected to be completed by mid-2018. These measures are collectively designed to deter, detect, delay, assess, communicate, and respond to potential physical threats to the whole facility.

4.3.2 Distribution Facility Protections

Distribution facilities are not subject to all NERC's CIP Reliability Standards as noted in Subsection 4.2.2. However, all FPL distribution and transmission substations have been protected by the standard set of substation security measures, which at a minimum include such protections as chain-linked fences, concrete vault with steel doors to house the relays, lighting, locks at the perimeter gate and the vault entrances. Where warranted, cameras are used in distribution substations based on perceived risks. Corporate Security uses portable cameras that are deployed to distribution substations as needed. FPL's Distribution Control Center uses a multi-layer security approach including a perimeter gate, badge readers, and cameras.

As noted, FPL's Facilities Management contractor is required to perform quarterly Substation Assessments for distribution substations. The Power Delivery business unit also conducts additional yearly substation condition assessments. FPL's field operations staff and engineering staff use a safety assessment checklist upon entering a substation to do work. This checklist includes a visual check for damage to the substation and the condition of the gate and fence.

4.4 Collaborative Resources

4.4.1 Industry Groups and Government Agencies

FPL maintains relationships with key industry partners to stay abreast of cybersecurity threats and research, remain current on physical and cyber security technology, and share best practices within the electric sector. FPL is engaged with these groups and agencies at all personnel levels.

Edison Electric Institute (EEI)

FPL participates in the EEI Spare Transformer Equipment Program (STEP). This program allows utilities throughout the country to find and share spare equipment in cases of emergency. Due to the long lead time for manufacture, transportation, and installation of large transformers, this program can substantially speed up recovery from physical attack.

UNITE

UNITE is an utility IT best practice sharing and benchmarking consortium led by utility Chief Information Officers. Companies have technology information to collectively increase IT maturity across utility member companies. FPL is a member and the IT Cyber Security program participates in order to improve FPL's cyber defenses.

NERC Electricity Information Sharing and Analysis Center (E-ISAC)

FPL also participates in the Cybersecurity Risk Information Sharing Program (CRISP). The program is managed by DOE and E-ISAC to facilitate the sharing of both unclassified and classified threat information. CRISP helps develop situational awareness tools that increase the electric sector's ability to prioritize and coordinate the protection of critical infrastructure.

Electric Power Research Institute (EPRI)

FPL is currently participating in an EPRI study to assess the potential electromagnetic pulse (EMP) impacts on the electric grid. This study will assess and provide guidance on system hardening and recovery and is to be completed by April 2019. FPL will then evaluate whether specific construction and protection specifications for their facilities are feasible to protect against EMP threats.

North American Transmission Forum (NATF)

The North American Transmission Forum is comprised of investor-owned, state-authorized, municipal, cooperative, U.S. federal and Canadian provincial utilities. It promotes reliability and resilience excellence of the electric transmission system. FPL's Vice President of Transmission and Substation sits on the Board of the NATF, and various other FPL employees participate in NATF's 12 industry practice groups.

Southeast Regional Domestic Security Task Force (SERDSTF)

The Regional Domestic Security Task Force serves as the foundation of the state of Florida's domestic security structure. The state is divided into several regions that each have their own RDSTF. The RDSTFs form the critical link between policy makers at the state level and the regional partners faced with the daily challenge of protecting the state's communities. It is co-chaired by the regional FDLE special agent in charge and one sheriff or police chief from the region. FPL's Sr. Director of Corporate Security is a member of the Executive Board of the Task Force. FPL's Senior Manager of Corporate Security is a member of the Critical Infrastructure

subcommittee, and the Corporate Intelligence Analyst is a member of the Intelligence subcommittee.

American Society for Industrial Security (ASIS)

ASIS International is a community for security practitioners from every industry in the public and private sector. Most members of the Corporate Security department are members and hold ASIS Professional Certifications. FPL attends the annual technology conference and participates with the utility subcommittee on best physical security practices.

International Security Management Association (ISMA)

ISMA consists of 400 Chief Security Officers, CEOs, and other delegates of major corporations across five continents. ISMA provides a trusted peer information-sharing network that companies use to benchmark across a wide variety of sectors on physical security issues. FPL's Senior Director of Corporate Security is an active member in the Critical Infrastructure subcommittee.

Local, State, and Federal Law Enforcement

FPL maintains contact with federal, state and local law enforcement, which provide information sharing to stay ahead of emerging threats. Some key partnerships include:

- Department of Homeland Security (DHS)
- DOE Electricity Subsector Coordinating Council (ESCC)
- FBI Joint Terrorism Task Force
- Fusion Centers

FPL's Corporate Security also works closely with local law enforcement serving as first responders to any emergency situation. Corporate Security has created a training film to help law enforcement understand its role and FPL's needs in responding to a suspicious situation at any of FPL's substations. This video will be presented to all law enforcement within the FPL service territory. Additionally, corporate Security has created a Law Enforcement guide book that describes the procedures of how to respond to a situation at a FPL substation.

4.4.2 Exercises and Assessments

Since 2016, FPL has conducted internal voluntary assessments and exercises to review and assess the adequacy of its physical and cyber security process and procedures.

GridEx IV

In November 2017, FPL took part as a full participant in GridEx IV. FPL believes that participation in these exercises enables the company to identify any gaps in security processes and leverage best practices across the industry. FPL is working on implementing lessons learned from this exercise into its plans and procedures.

Internal Physical Security Drills

FPL conducts yearly physical security table top exercises around its service territory at CIP-014 substations. FPL invites federal and state agencies such as the FBI, the Department of Homeland Security, and the Florida Fusion Center to attend as well as local law enforcement. An operational, safety, and security review of each location is performed to ensure that local law

enforcement understands the optimal course of action if there is a threat at these substations. The company uses two threat scenarios during these table top exercises.

Internal Cyber Security Drills

FPL's Cyber security department performs periodic tabletop cyber drills involving critical business units such as transmission and distribution. These drills allow the company to test its Cyber Security Incident Response Procedure and update the document with any lessons learned. FPL conducts an annual Corporate Cyber Drill to assess the company's response to a cyber and physical event. All levels of personnel are incorporated. This drill has used threat scenarios such as phishing, malware, data breach, and rolling blackouts.

Cybersecurity Capability and Maturity Model (C2M2)

In 2016, the company used a third-party vendor to perform the Electric Subsector Cybersecurity Capability and Maturity Model (C2M2). FPL's Cyber Security department integrated the recommendations and lessons learned from the C2M2 assessment.

4.4.3 Audits

FPL performed internal audits pertaining to cyber security controls, assessments, and network penetration tests in 2014 and 2015. All mitigating actions and improvements have been completed.

The Cyber security department engages cybersecurity service providers and consultants to assess the adequate deployment of controls, tools, and processes of the FPL's cybersecurity. Recommendations help the company improve the overall effectiveness of cybersecurity measures. Annually, FPL uses several third-party service providers to perform testing and assessments. The FRCC, with delegated authority from NERC, conducts periodic audits, self-certifications, and spot checks to assess FPL's compliance to the NERC standards.

4.5 Incident Reporting, Response, and Recovery

4.5.1 Reporting and Response Planning

As part of NERC CIP-008 and EOP-004, FPL is required to develop specific plans and procedures for reporting and responding to a cyber or physical incident affecting the BES Cyber System. Additionally, in case of a cyber or physical security incident, the company engages other entities in their reporting and response process.

North American Electric Reliability Corporation (NERC)

FPL's *Cyber Security Incident Response Procedure* documents the plan for identifying, analyzing, responding to, and reporting a cyber-security incident involving High, Medium, and Low Impact BES cyber systems. The *Cyber Security Incident Response Procedure* serves as a module under the Corporate Emergency Management Plan. This plan applies to all NextEra Energy's BES Cyber Systems, its associated cyber assets, and information. This plan is required to be reviewed annually.

As required by EOP-004, FPL's *Notification and Event Reporting Procedure (EOP-004-3)* describes the processes for recognizing and responding to disturbances and unusual occurrences

that are suspected to be sabotage or vandalism at NextEra Energy facilities. This document establishes the procedures to report incidents both internally and to external agencies. The plan is to be reviewed by FPL personnel annually.

Additionally, operating employees receive annual Security Notification and Event reporting training through the FPL Learning Management System. This training focuses on recognizing suspected sabotage or vandalism and the process of responding through the reporting structure.

Department of Energy (DOE)

The Department of Energy requires companies to file Form OE-417 to report any electronic incidents and disturbances such as might be triggered by a physical or cyber attack. The form requires a description of the incident, the cause of the disturbance, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. Since 2014, FPL has reported three security incidents to the DOE via form OE-417.

Florida Department of Emergency Management (FDEM)

In case of a cyber or physical attack that cause a widespread outage, FPL's Director of Emergency Preparedness would consult with FPL leadership and contact the duty officer at FPL's State Watch Office in Tallahassee. The duty officer would then notify the FDEM.

Florida Public Service Commission

In case of a cyber and physical security incident resulting in impacts such as described in Rule 25-6.018 F.A.C., FPL states that the company's Regulatory Affairs group would be in contact with the Commission. Under these circumstances, FPL's protocols would include contact with other government agencies such as FDEM and the Governor's office.

Local, State, and Federal Law Enforcement

In case of a physical security incident, FPL's Security Operations Center would serve as a point of contact for any law enforcement.

4.5.2 Recovery Planning

NERC Reliability Standards such as CIP-009, EOP-005, EOP-008, and EOP-011 contain recovery and restoration planning requirements.

As required by CIP-009, FPL also maintains separate recovery plans for each of the functioning areas that support High and Medium Impact facilities. Low Impact and distribution facilities are not required to have specific plans. The company states that it uses best utility practice recovery methods and processes.

Pursuant to EOP-005, FPL reports it has developed and implemented the required plan detailing system restoration following a disturbance in which one or more areas of the BES system shuts down and the use of Blackstart Resources are required. FPL's *System Restoration Plan for Interconnection and Blackstart Procedures* provides the switching procedures and high level strategy to help in the restoration process following an event that leads to either a total or partial blackout of the FPL system.

As required by EOP-008, the company must develop an operating plan in case the primary control center functionality is lost. FPL's *Loss of Control Center Functionality System Operating Procedure* assists the company in continuing reliable operations of the BES via the Backup Control Center in the event that the primary control center becomes inoperable or impaired.

Pursuant to EOP-011, FPL is required to develop and implement operating plans and procedures to mitigate emergency situations. FPL states that it is in compliance with these NERC EOP Standards. *FPL Emergency Plan for Capacity Shortages/Transmission Limitations and Long Term Fuel Shortages* provides the policies and procedures used by FPL in responding to a power capacity shortage or transmission limitation which impacts or could impact service to a significant number of customers.

4.6 Cyber and Physical Security Cost Tracking

FPL has implemented no new initiatives to track physical security costs of its substations and control centers. The company continues to track certain physical security costs in Corporate Security Capital and O&M budgets. These costs include card readers, card access controllers, and cameras. However, some physical security costs are shared with other operational business units. For example, the cost of new security equipment is included in the cost of a new substation. FPL also tracks cybersecurity costs within the IT Cyber security department budget at the enterprise level. Examples of these types of costs include dedicated cyber security labor, firewalls, logging and alerting tools, intrusion detection systems, and cyber security assessments.

5.0 Gulf Power Company

Gulf Power Company (Gulf) is a subsidiary of Southern Company and serves 455,415 residential and commercial customers in northwest Florida. It is a vertically integrated utility producing 2,277 MW with generation, transmission and distribution capacities monitored by two control centers. Its system includes 135 substations: 77 distribution, 27 transmission, and 31 that are dual transmission and distribution. Sixty-two substations are designated as BES substations operating at or above the FERC "bright-line" threshold of 100 kV. Gulf is a member of the SERC Reliability Corporation, one of eight regional reliability councils under NERC.

5.1 Organization

Gulf collaborates with Southern Company to meet enterprise goals using cross-functional teams, committees, liaisons, and shared policies and procedures throughout its organization. Gulf uses internal resources and those from its parent company to plan, manage, and update cyber and physical security policies, protections, and compliance activities.

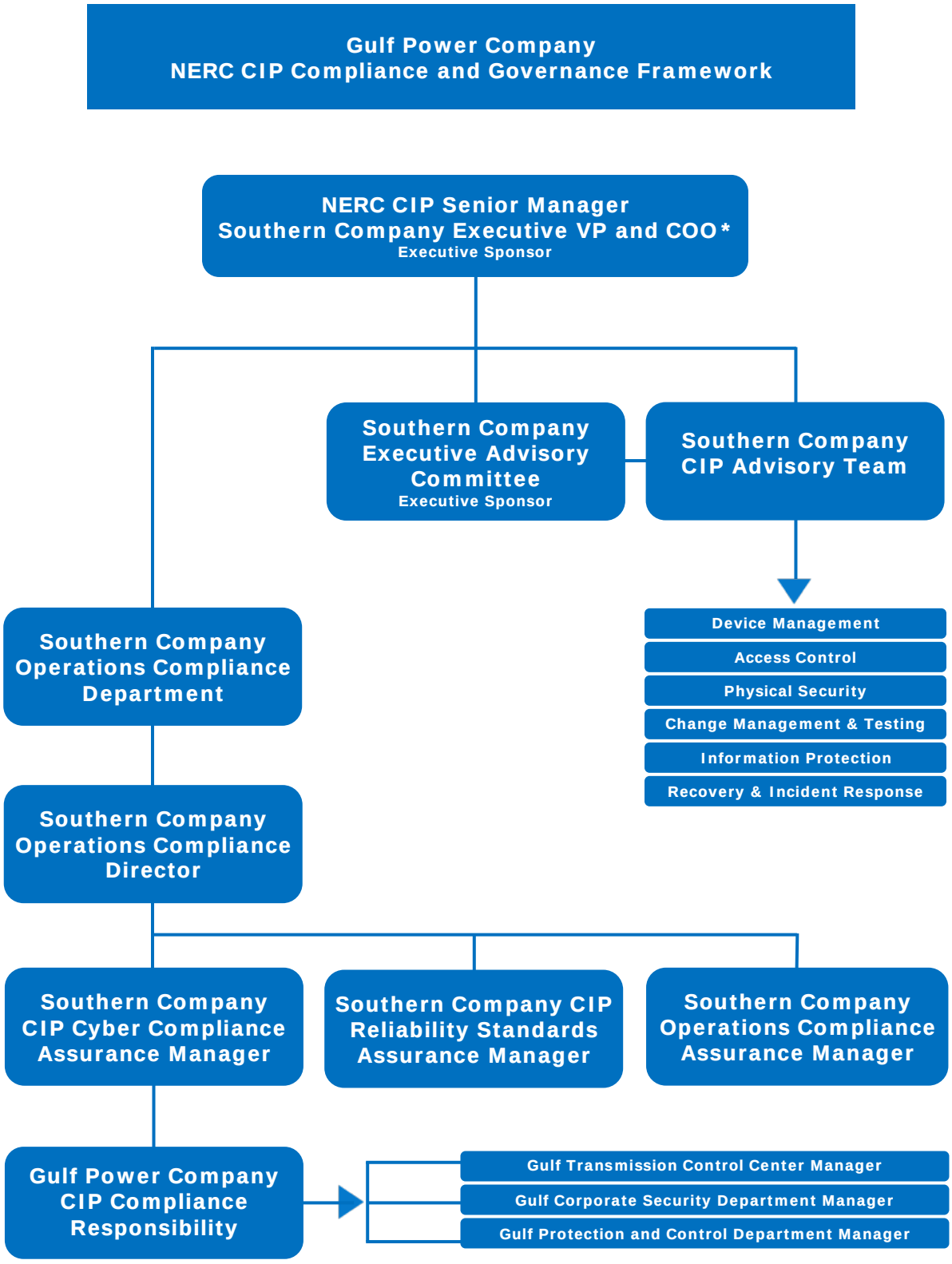
5.1.1 CIP Senior Manager – Executive VP & Chief Operating Officer

NERC requires that each utility designate a CIP Senior Manager to oversee CIP compliance. According to CIP-003, Requirement 3, "the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011." The Executive Vice President and Chief Operating Officer of Southern Company is the designated CIP Senior Manager for Southern Company and all its affiliated utilities, including Gulf. The CIP Senior Manager delegates specific compliance responsibilities to Southern Company Services (SCS).

5.1.2 Southern Company Services Operations Compliance Function

The Gulf NERC CIP compliance framework is integrated with Southern Company Services. The executive department charged with CIP compliance is the SCS Operations Compliance department. This department is independently responsible for CIP regulatory oversight, implementation, management, and monitoring of Southern Company operating companies.

The SCS Operations Compliance department oversees CIP implementation and compliance reporting for CIP-002 through CIP-014. The department is led by the Compliance Director who oversees three CIP assurance managers focusing respectively on the Reliability Standards, operations compliance, and cyber compliance. These managers are delegates of the CIP Senior Manager. The Cyber Compliance Assurance Manager provides CIP compliance support to Gulf Power Company. **Exhibit 5** depicts the Southern Company and Gulf CIP compliance and governance framework.



*Chief Operating Officer

Exhibit 5

Source: Document Request Responses 2 and 3.14

Gulf relies on the Southern Company compliance and governance framework to adhere to the CIP Reliability Standards. The framework is sponsored at the executive level by the Southern Company CIP Senior Manager and Executive Advisory Committee.

5.1.3 Executive Advisory Committee

The Executive Advisory Committee includes Southern Company senior personnel from legal, technology, compliance, energy management systems, and transmission functions. Subordinate to the NERC CIP Senior Manager and the Executive Advisory Committee is a CIP Advisory Team comprised of managers responsible for CIP compliance, physical security, and cybersecurity at Southern Company and its operating companies.

5.1.4 CIP Advisory Team

The CIP Advisory Team is responsible for developing Southern Company CIP compliance and implementation policies. The CIP Advisory Team guides and directs subordinate policy development teams and CIP Implementation Steering Committees on policies and work practices. Gulf management describes the steering committees as subject matter experts and boots on the ground for CIP compliance, control centers, information systems, generation, and substations. Gulf personnel serve on the applicable steering committees. At the company level, Gulf implements CIP requirements through its Corporate Security department, Transmission Control Center, and Protection and Control department.

A centralized Security Operations Center, staffed by personnel from the Southern Company Services IT Security department, provides around-the-clock cybersecurity overwatch of network traffic, monitoring all Southern Company CIP Medium Impact substations and transmission and distribution assets. Additional responsibilities include sharing cybersecurity initiatives and best practices with Gulf and other operating companies.

Southern Company uses a cross-functional physical security core team at the enterprise level to manage transmission physical security. This team is responsible for securing transmission assets using planning and risk analysis, spare parts and equipment, physical security, security intelligence, and communications and response. This team includes personnel from Gulf, Southern Company, and other operating companies and the team partners with Southern Company transmission, distribution, generation, policy, compliance, and IT resources.

The Southern Company Security Council monitors and secures operating companies' assets. The council is comprised of operating company managers and directors who provide expertise in risk management, business assurance, operations compliance, IT security, transmission maintenance, technology, and application development. The coordinators are the CIP Security Operations Manager and Transmission Coordinator/Investigations Supervisor.

The Gulf Corporate Security Manager is a core member of the Southern Company Security Council and responsible at the operating company level for physical security of Gulf transmission and distribution facilities, generating plants, and the corporate office. The manager leads a team of investigators charged with physical protection of facilities and related security issues.

5.1.5 Policies and Procedures

Southern Company policies and procedures provide the implementation structure for Gulf CIP compliance and overall cybersecurity protection. The Southern Company *NERC CIP Cyber Security Policy* directs compliance with CIP-002 through CIP-011 for cyber and physical security requirements for all High, Medium, and Low Impact BES Cyber Systems. The NERC CIP Senior Manager last reviewed and approved this policy in June 2017.

The Southern Company *NERC CIP Procedures Manual* is electronically available to Gulf employees via an intranet. It contains a list of CIP requirements, procedures, and resources covering program administration, access control, change management, testing, device management, information protection, physical security, recovery, and incident response. Southern Company's Policy Development team drafts and publishes the procedures for the *NERC CIP Procedures Manual*.

As summarized in Chapter 2, Gulf is subject to EOP and TPL requirements. Gulf shares responsibility with Southern Company for oversight, implementation, and compliance. Southern Company Services has specific responsibility for compliance with EOP-006, EOP-008, EOP-010, EOP-011, and TPL-001. Gulf shares responsibility with SCS for EOP-004, EOP-005, and TPL-007 compliance.

The Southern Company Corporate Security Council receives updates on physical security policies and work practices created by the CIP governance team through the Security Director of Alabama Power Company, an operating company of Southern Company. The Security Council is required to teleconference monthly and to meet quarterly, sharing information about threats that may affect critical infrastructure. Besides these scheduled requirements, council members exchange information electronically or telephonically as needed.

According to Gulf, the Southern Company Transmission and Distribution Cybersecurity Program uses NIST-based policies and procedures for strategic, operational, and tactical planning and management of cyber risk outside of NERC CIP requirements. Program procedures and practices designed to limit risk include:

- Compartmentalization/network zoning to prevent unauthorized access to secure networks
- Layered defenses to reduce the potential impact of cyber attacks
- Separation of duties and least-privilege limitations
- Continuous centralized monitoring of company networks to respond to cyber threats

The Gulf Corporate Security department is responsible for implementing procedures related to physical security. These procedures include access control, security training, investigations, personal protection, uniform security, and law enforcement outreach.

Law enforcement outreach enables establishing, maintaining, and exercising contact with local, state and federal law enforcement agencies. The Corporate Security department also performs site-specific risk evaluations to assess facility physical security needs beyond those established by the CIP requirements.

The Gulf Corporate Security Business Assurance department is responsible for and governs critical facility operations during emergencies. The *Business Assurance Policy* provides the procedural framework for these operations.

5.2 Cybersecurity Protections

Gulf completed CIP Version 5 requirements for Medium and High Impact Cyber Systems prior to July 2016 and for Low Impact Cyber Systems before April 2017. Gulf reports that CIP Version 6 requirements for Low Impact assets are on track for implementation before the September 2018 deadline.

As required by CIP-002, Gulf has evaluated its assets and categorized each as High, Medium, or Low Impact in relation to the Bulk Electric System. To comply with CIP-003, Gulf's security management controls program covers the documentation, approval, and implementation of the *NERC CIP Cyber Security Policy*. This policy impacts all BES Cyber Systems within the scope of the CIPs.

5.2.1 Transmission

Included in the Gulf BES are 27 transmission and 31 dual transmission/distribution substations. If the Bulk Electric System is disrupted, the effects may be significant and widespread beyond Southern Company territories.

CIP Version 5 expanded protections to all BES Cyber Systems at critical facilities and requires utilities to safeguard these systems. Version 5 requires utilities to identify each critical asset as a High, Medium, or Low Impact BES Cyber System and applies specific protections to High and Medium Cyber Systems. Similar protections for Low Impact assets were not defined until January 2016 by CIP-003 Version 6. The new requirements for Low Impact Cyber Systems address cybersecurity awareness, physical security controls, electronic access controls, and cybersecurity incident response.

Gulf states that it has implemented CIP Version 5 cybersecurity controls and protections for all High and Medium Impact BES Cyber Systems. For Low Impact BES Cyber Systems, Gulf states it has implemented most required security controls and it will complete these actions before the CIP-003 Version 6 deadline of September 1, 2018.

Personnel & Training

As part of the personnel risk requirement in CIP-004, unescorted contractors, vendors, and Gulf personnel with access to High and Medium Impact BES Cyber Systems or related assets must undergo a risk evaluation. Included in this evaluation are an identity verification and criminal background check that recurs every seven years.

Employees and contractors with physical or electronic access to High or Medium BES Cyber Systems or associated systems receive annual training through Gulf's cybersecurity awareness program. All personnel with access to BES Cyber Systems also receive a quarterly cybersecurity newsletter.

The SCS Operations Compliance department administers a cybersecurity training program mandating CIP training for personnel with physical or electronic access to High or Medium Impact BES Cyber Systems or related cyber assets. Personnel are required to complete training prior to accessing these systems and to repeat the training annually.

As part of CIP-011, the Gulf access management program includes policies permitting, managing, and rescinding access to High and Medium Impact BES Cyber Systems or related assets. Personnel requesting electronic access to these systems or physical entry at a CIP physical security perimeter must be approved. Each approval defines the limits of individual access.

Outside of NERC CIP requirements, Southern Company's Transmission and Distribution Cybersecurity Program implemented a security awareness initiative that separates duties and least-privilege. This separation limits individual employee access within cyber systems, including Low Impact substations.

To reduce personnel risk, Southern Company also operates an Insider Threat Fusion Center comprised of analysts and IT specialists to monitor employees, contractors and vendors for malicious activity. When required, the activity is escalated to the interdisciplinary Southern Company Insider Threat Working Group, who can recommend further investigation through the appropriate operating companies.

Electronic Access

Gulf is required by CIP-005 to safeguard High and Medium Impact BES Cyber Systems that are connected to a network within an electronic security perimeter. Safeguards include firewalls, protocols for inbound and outbound traffic, and detection of malicious communications. The electronic security perimeter management procedure covers operations, maintenance, and decommissioning of ESPs. Gulf's High and Medium Impact BES Cyber Systems are connected to a network with a routable protocol within an electronic security perimeter. Gulf states that the company will implement required Low Impact controls by the deadline of September 1, 2018.

System Security Management

Gulf uses a cyber system management procedure to organize maintenance of CIP Cyber Systems into a lifecycle format covering planning, commissioning, operating, and decommissioning. These procedures are intended to prevent malicious code intrusion and to secure ports, services, accounts and patches for High and Medium Impact BES Cyber Systems. Although CIP-007 does not protect Low Impact systems, Gulf extends cybersecurity protections to all substations via its Transmission and Distribution Cybersecurity Program.

Change Management and Vulnerability Access

Gulf's change management procedure governing High and Medium Impact BES Cyber Systems describes change authorization, change testing and controls checks, and baseline documentation updates. The *Baseline Configuration Change Management Work Practice* covers personnel roles, compliance requirements, scope and processes. Gulf's BES Cyber System Management Program describes vulnerability assessments for BES Cyber Systems and related assets, including scheduling, action plans, and status tracking. Although CIP-010 specifically applies to High and Medium Impact BES Cyber Systems, Gulf's Transmission and Distribution Cybersecurity Program also protects Low Impact assets.

For CIP-011, Gulf maintains an information protection program to safeguard BES Cyber System information for High and Medium Impact BES Cyber Systems and a CIP access management program to record, limit, and identify authorized administrators. These programs include guidelines for protecting BES Cyber System information prior to disposal or repurposing data storage devices. For all substations including Low Impact Cyber Systems, Gulf relies on the Transmission and Distribution Cybersecurity Program to protect sensitive data.

Proposed NERC Standards

As of report publication, CIP-012 and CIP-013 are both pending NERC approval. Southern Company has participated in the drafting process for CIP-012, submitting feedback regarding the scope and implementation of the proposed standard.

Gulf managers believe existing procedures adequately address the proposed requirements of CIP-013. Gulf uses *Supply Change Management Policies and Procedures*, the *Technology Acquisition Policy*, and a third-party security standard to manage supply chain risk. Gulf is coordinating its CIP-013 implementation plan with the Southern Company Director of Strategic Sourcing.

Transmission and Distribution Cybersecurity Program

In 2012, Gulf created the Transmission and Distribution Cybersecurity Program, which Gulf describes as voluntary and meeting or exceeding CIP requirements. The program manages cyber transmission and distribution asset risk using monitoring, access restrictions, compartmentalization, and layered defenses. The program consists of four initiatives:

- Detection and Monitoring
- System and Communication Protection
- Identity Management and Access Controls
- Configuration Management and Media Protection

Detection and Monitoring efforts were completed in 2016. These efforts are intended to improve capabilities to detect cyber attacks on transmission and distribution substations or other critical infrastructure. Gulf implemented System and Communication Protection in 2017, which employs firewalls and manages switches to secure network access. Identity Management and Access Controls is designed to limit personnel access based on job scope and will be completed by 2020. Configuration Change Management and Media Protection improvements will scan files and protect media, and are scheduled to be completed by 2020.

5.2.2 Distribution

Utility distribution systems are not within the scope of the protections of the CIP Reliability Standards. However, Gulf states its elective cybersecurity policies and procedures provide added protections for systems that monitor and remotely control distribution facilities. These protections are part of the Transmission and Distribution Cybersecurity Program, which, according to Gulf, extends cyber protections to all substations and related cyber systems, regardless of voltage class.

Gulf provides classroom and/or on-the-job training to personnel with access to distribution cyber assets. This training is scaled to each employee's level of cyber access. This instruction includes cybersecurity awareness and technical details of specific distribution cyber assets.

5.3 Physical Security Protections

5.3.1 Transmission Facility Protections

CIP-006 and CIP-014 impose specific physical security requirements intended to protect critical cyber assets and substations. Gulf uses a combination of these mandatory actions and voluntary company initiatives, employing layered safeguards for its substations. The Gulf Corporate Security Manager oversees these efforts to deter, detect, and delay potential intruders.

CIP-006 Version 6 requires Gulf to have a documented physical security plan to protect High and Medium BES Cyber Systems associated with control centers, transmission stations and substations, and control houses. Specific requirements apply to High Impact BES Cyber Systems and to Medium Impact BES Cyber Systems with external routable connectivity. Low Impact BES Cyber System protections will be implemented by September 2018. Gulf affirms it is on track to meet this deadline.

For CIP-006, Gulf established a physical security program and a physical access control system restricting and logging facility access for personnel working in or near High and Medium Impact BES Cyber Systems. Gulf has no substations meeting the criteria for High Impact BES Cyber Systems but the company has implemented CIP-006 substation controls for Medium Impact BES Cyber Systems. For these stations, Gulf employs protections including interior and exterior proximity badge readers, code door locks, motion sensors, and visitor logs. Protections for Physical Access Control Systems associated with High and Medium Impact BES Cyber Systems may also include badge readers, biometric scanners, backup door code locks, motion sensors, alarms, and physical barriers at openings. In addition, Gulf has added thermal cameras and monitoring tools capable of distinguishing between animal and human activity.

For Low Impact substations, Gulf uses networked cameras, exterior proximity badge readers, and code door locks. As of January 2018, 40 percent of Low Impact substations were equipped with proximity badge-based access control systems. The Gulf Power Security Control Room provides central monitoring for all CIP and non-CIP alarms and cameras. It is staffed 24 hours a day and reports to the Gulf Corporate Security Manager.

After the 2013 Metcalf substation attack, CIP-014 was implemented to improve physical security at critical transmission stations or substations that if damaged, could result in widespread instability, uncontrolled separation, or cascading outages. CIP-014 requires transmission owners to conduct recurring risk assessments to identify key transmission stations and substations and the primary control center responsible for each transmission station or substation. An independent third-party must verify the risk assessment.

In response to the Metcalf attack, the Gulf Corporate Security department modified its physical security approach and scope to include areas outside substation perimeters. Gulf states it has increased its field of vision around substations.

In 2017, Southern Company Services performed a risk analysis of current Gulf facilities and those scheduled to be in service within 24 months. The analysis included a review of steady state power flow, stability, and frequency excursions. A third-party verified this risk analysis. Gulf states it has no transmission stations or substations, or primary control centers that are subject to CIP-014 Requirements 4, 5, and 6. These provisions include developing a physical security plan, communicating with law enforcement, and evaluating potential physical threats, among others.

In recent years, Gulf placed emphasis on training and liaisons with law enforcement. As part of this initiative, Gulf security investigators are required to build relationships with local, state and federal agencies. The Corporate Security department trains law enforcement to recognize suspicious activity at substations.

Gulf Corporate Security investigators perform a routine, site-specific, risk-based assessment on all substations. Assessments estimate the probability of intrusion, identify substation vulnerabilities, develop and prioritize remediation, and assess threats directed at specific facilities. Investigators also evaluate national level threats and those directed at Southern Company or Gulf. Other assessment criteria include site location (urban vs. rural), distance from law enforcement, local criminal activity, security case logs, existing safeguards, and the criticality of each facility. The Gulf Corporate Security department states that it updates physical security procedures in response to assessment findings. Investigators update security protections as needed in response to threats, site conditions, regulatory changes, or when current protections are determined to be insufficient and inadequate. The most recent assessments took place in January and February 2017, and did not identify any shortcomings or needed improvements.

5.3.2 Distribution Facility Protections

Although distribution-only substations do not fall under the scope of NERC CIP requirements, Gulf states it conducts routine risk-based, site-specific assessment on all distribution and transmission substations. In conjunction with the risk assessment, Gulf employs these physical precautions for distribution substations and equipment:

- Installation of perimeter fencing and cameras at the distribution control center
- Annual inspection of pole mounted distribution reclosers
- Annual inspection of distribution control cabinet security locks
- Addition of badge access systems in substations with distribution equipment
- Addition of badge access systems to non-BES substations as they are built or upgraded

5.4 Collaborative Resources

5.4.1 Industry Groups and Government Agencies

NERC and North American Transmission Forum

Southern Company is actively involved with energy sector associations and government agencies. Collaborations include interaction with the NERC Electricity Information Sharing and Analysis Center and participation in the NERC regional committee, focus groups, and pilot programs for CIP Versions 5 and 6 implementations. Southern Company also participates in NATF practice group meetings and webinars, which contribute to the development of related policies.

Electric Power Research Institute

Southern Company and Gulf participate in EPRI research on transmission planning, system protection, generation, and other areas. The President of Southern Company serves on the EPRI Board of Directors and employees from Gulf and Southern Company serve on over 200 EPRI committees. Management believes that Southern Company and its operating affiliates benefit from EPRI's extensive research and development portfolio, gaining insight and understanding of new technology and data analytics.

To research electromagnetic pulse and its risks to grid reliability and recovery, Southern Company is actively tracking a three-year EPRI study on high altitude electromagnetic pulse. To understand vulnerability to geomagnetic disturbances, Southern Company collaborates with EPRI, NASA, IEEE, and other utilities. Southern Company added geomagnetically induced current monitors to its research systems and supported NASA's installation of a magnetometer on the Southern Company footprint.

Spare Transformer Equipment Program

Gulf is a member of the Spare Transformer Equipment Program, an industry program formed in 2006 to strengthen electrical sector ability to restore the transmission system following a potential physical attack. Each participant is required to maintain a certain number of spare transformers and, if necessary, to sell these spares to any other member that experiences acts of deliberate, documented terrorism, as defined in the Homeland Security Act of 2002, resulting in:

- Destruction or long-term disabling of one or more electric transmission substations, and
- Declaration of a state of emergency by the President of the United States pursuant to the National Emergencies Act.

Department of Energy - CRISP

Southern Company and Gulf are active members of CRISP, a voluntary program deployed by DOE to facilitate exchange of cybersecurity information. CRISP helps secure critical networks from sophisticated cyber threats by employing passive devices to collect and transmit cyber information. CRISP integrates cyber-related threat information from government agencies with the analysis from member utilities.

Department of Homeland Security – Cyber Sharing

Gulf participates in the Cyber Information Sharing and Collaboration Program, a part of the Department of Homeland Security's National Cybersecurity and Communications Integration Center. The program is a cyber threat information sharing effort between government and the private sector. Member companies share information, which is then analyzed and distributed to participants in a non-attributable format via bulletins, reports, alerts, and guidelines for best practices.

Third-Party Cyber Partners

Gulf enhances its cybersecurity protection by contracting with several third-party cybersecurity vendors. These companies collect and/or share information such as:

- Data on threats targeting industrial control systems and best practices for detection, prevention, response, and recovery for these systems;
- Actionable intelligence about external cyber threats from phishing schemes, domain theft, social media activity, mobile apps, impersonation attempts, and marketplace fraud; and,
- Predictions on insider threats and supply chain risks derived from data analytics and human analysis of the deep and dark webs

Law Enforcement

To prevent physical attacks on substations, the Gulf Corporate Security department receives information from government agencies and investigators reach out to local law enforcement. These information sharing resources include Tallahassee and Escambia Fusion Centers, FBI, InfraGard, Florida Department of Law Enforcement, Regional Domestic Security Task Force, and liaisons from the Pensacola Police Department and sheriffs' offices in Escambia and Santa Rosa counties.

5.4.2 Exercises and Assessments

NIST Cybersecurity Capability Maturity Module – ES-C2M2

In 2012, Gulf worked with the IT Security department of Southern Company Services to complete a cybersecurity assessment using criteria from the National Institute of Standards and Technology. According to Gulf, the assessment findings spurred the development of the Transmission and Distribution Cybersecurity Program. In 2015, Gulf evaluated the maturity of this program using the Electrical Sector Cybersecurity Capability Maturity Model (ES-C2M2), a tool from the Department of Energy based on the NIST cybersecurity framework. Gulf states that it reviewed the 2015 findings and addressed gaps in its development plan.

In 2014, Gulf applied the ES-C2M2 to ten domains including risk management, threat and vulnerability management, situational awareness, incident response, workforce management, and cybersecurity program management. The assessment recommended changes to situational awareness. In November 2017, Gulf performed a new ES-C2M2 assessment and the results are pending. Gulf management states that it expects an improvement in situational awareness as a result of updating initiatives within the Transmission and Distribution Cyber Security Program.

GridEx IV

In November 2017, Gulf employees participated as observers at GridEx IV, a two-day simulated physical and cybersecurity attack exercise coordinated by NERC. Southern Company states it used GridEx to improve coordination and communication, review incident response plans, engage leadership, and identify areas for improvement among its operating companies. Commission audit staff reviewed Gulf's GridEx IV lessons learned.

Southern Company Threat Modeling

Gulf employs threat modeling after newsworthy third party cyber incidents. After the attacks on the Ukrainian electrical grid in December 2015, SCS IT Security reviewed critical networks and NERC industry recommendations. In 2016 and 2017, Gulf and Southern Company used threat modeling after the ransomware attacks in Ukraine for post-event analyses. These efforts helped identify attackers' techniques and critical paths within the enterprise. In response to this new information, Southern Company IT revised its policies and remediation timelines, added multifactor identification and cyber incident response plans for DSCADA and EMS, segmented facility control systems, and reported its findings to NERC.

IronNet

Southern Company is a sponsor of the IronNet Cybersecurity pilot. IronNet uses multiple data points to identify potential cyber attacks. These points are derived from observation of threat actors attempting to target and penetrate cyber assets. IronNet analyzes enterprise data activities in real time then shares the analytics and threat data. The intent of this rapid information exchange and cross-sector collaboration is to enable a collective threat response. Southern Company states it intends to use IronNet to detect internal cyberattacks, such as unauthorized access of secure networks or malicious activity.

Idaho National Labs

Southern Company is participating in a new pilot program directed by Idaho National Labs designed to create security architecture that detects and shares information about cyber threats aimed at operational technologies. This pilot will use the Southern Company Transmission and Distribution Detection and Monitoring initiative as its model.

PhishMe Campaign

Gulf engages in a quarterly internal PhishMe Campaign to improve awareness of cyber risks in the workplace. The campaign sends employees suspicious emails and monitors click-through rates. Gulf employees who frequently click on suspicious links are required to undergo additional training.

Gridwatch

Gulf and other operating companies within Southern Company developed and participate in Gridwatch, a video training tool for employees and law enforcement. The program shows law enforcement how to identify criminal activity at facilities and encourages employees to report suspicious activity.

5.4.3 Audits

The SERC Reliability Corporation performed a CIP compliance audit of Southern Company Transmission and Gulf Power Company from July to October 2016. The audit covered operation,

controls, policies, practices, and procedures for physical and cybersecurity at transmission substations, generation facilities, and control centers for all applicable CIP Reliability Standards. The 2016 SERC audit reported no findings.

5.5 Incident Reporting, Response, and Recovery

5.5.1 Reporting and Response Planning

Under EOP reporting requirements, Gulf has experienced no security incidents requiring an EOP-004-3 report or Department of Energy OE-417 submittal since 2014.

Gulf is subject to specific reporting requirements from Florida Public Service Commission Rules 25-6.018 and 25-6.019. They mandate that regulated utilities notify the Commission under specific circumstances which threaten the bulk power supply integrity or result in loss of service. After a cyber or physical attack, Gulf management plans to contact the Commission if such an incident resulted in a qualifying interruption of service.

As required in CIP-008, Gulf deploys an incident response plan to safeguard High and Medium Impact BES Cyber Systems. This plan includes personnel roles and procedures to identify, categorize, report, and respond to cyber attacks. Gulf also has policies to update and evaluate this plan by performing incident response drills. Gulf management states these exercises are performed alongside Southern Company affiliates to test incident responders and identify areas for improvement. The most recent incident response drill for High and Medium Impact BES Cyber Systems occurred during GridEx IV in November 2017.

Although CIP-008 pertains to High and Medium Impact BES Cyber Systems, Gulf is also required to maintain a cybersecurity plan with regular reinforcement for Low Impact BES Cyber Systems. In parallel with these requirements, Gulf states the Southern Company Transmission and Distribution Cybersecurity Program is implementing incident response procedures for all substations.

In addition to these protections, Gulf employs two monitoring stations providing system oversight and incident response protocols at both operating utility business and enterprise levels. Gulf's primary station is located in Florida and the backup is in Alabama. Redundancies are incorporated into the communications structure across both systems in the event that either station is compromised.

Gulf Corporate Security develops contact protocols with multiple local, state, and federal agencies. When suspicious activity is discerned, law enforcement responds and notifies Corporate Security.

The Corporate Security Incident Response team periodically conducts active shooter drills to train employees to appropriately respond to hostile intruders. The Corporate Security department evaluates the performance of the Incident Response team. As a result of feedback from this drill, Gulf has upgraded its physical security measures. The last drill was held March 2018.

5.5.2 Recovery Planning

In accordance with CIP-009, Gulf has developed recovery plans for High and Medium Impact BES Cyber Systems, electronic access control and monitoring systems, and physical access control systems. These plans describe personnel roles, conditions for activation, and processes for validating and updating the plans.

Gulf also engages in Southern Company recovery drills. The last recovery drill took place in June 2017 for High Impact BES Cyber Systems. Although Medium Impact BES Cyber Systems at Control Centers are subject to one or more testing requirements under CIP-009, Gulf has no control centers that meet these criteria. For Low and Medium Impact substations outside the scope of CIP-009, Gulf states it is implementing recovery plans as part of the Transmission and Distribution Cybersecurity Program.

EOP-005 is a shared responsibility between Gulf and Southern Company Services. EOP-005 requires that plans, facilities, and personnel are prepared to maintain grid reliability when restoring systems and the Interconnection. As a Transmission Owner with a blackstart resource, Gulf is subject to Requirement 11 and must have written blackstart resource agreements with testing protocols. SCS is subject to the other provisions of EOP-005.

EOP-008 and EOP-011 are applicable to Reliability Coordinators, Balancing Authorities, and Transmission Operators. Southern Company Services performs these functions on behalf of Gulf and maintains compliance with both procedures.

The Gulf *Business Assurance Policy* provides guidelines for business operations in an emergency. This policy requires that business units develop recovery plans for continued operations following an unplanned interruption.

5.6 Cyber and Physical Security Cost Tracking

In the Commission's 2014 report, audit staff reviewed the corporate security budgets for security costs. Staff noted that these costs were embedded into operating and project budgets, making it challenging to develop a complete understanding of all physical security costs.

Since 2014, Gulf has isolated more of its physical, cyber, and regulatory capital costs. At the plant level, Gulf tracks costs for cyber and physical security initiatives related to CIP Reliability Standards. Gulf separates non-CIP cyber and physical security costs. Gulf uses engineering work orders to track operations and maintenance work related to physical and cybersecurity programs. A breakdown of Gulf capital spending from 2014 to November 2017 is shown in **Exhibit 6**.

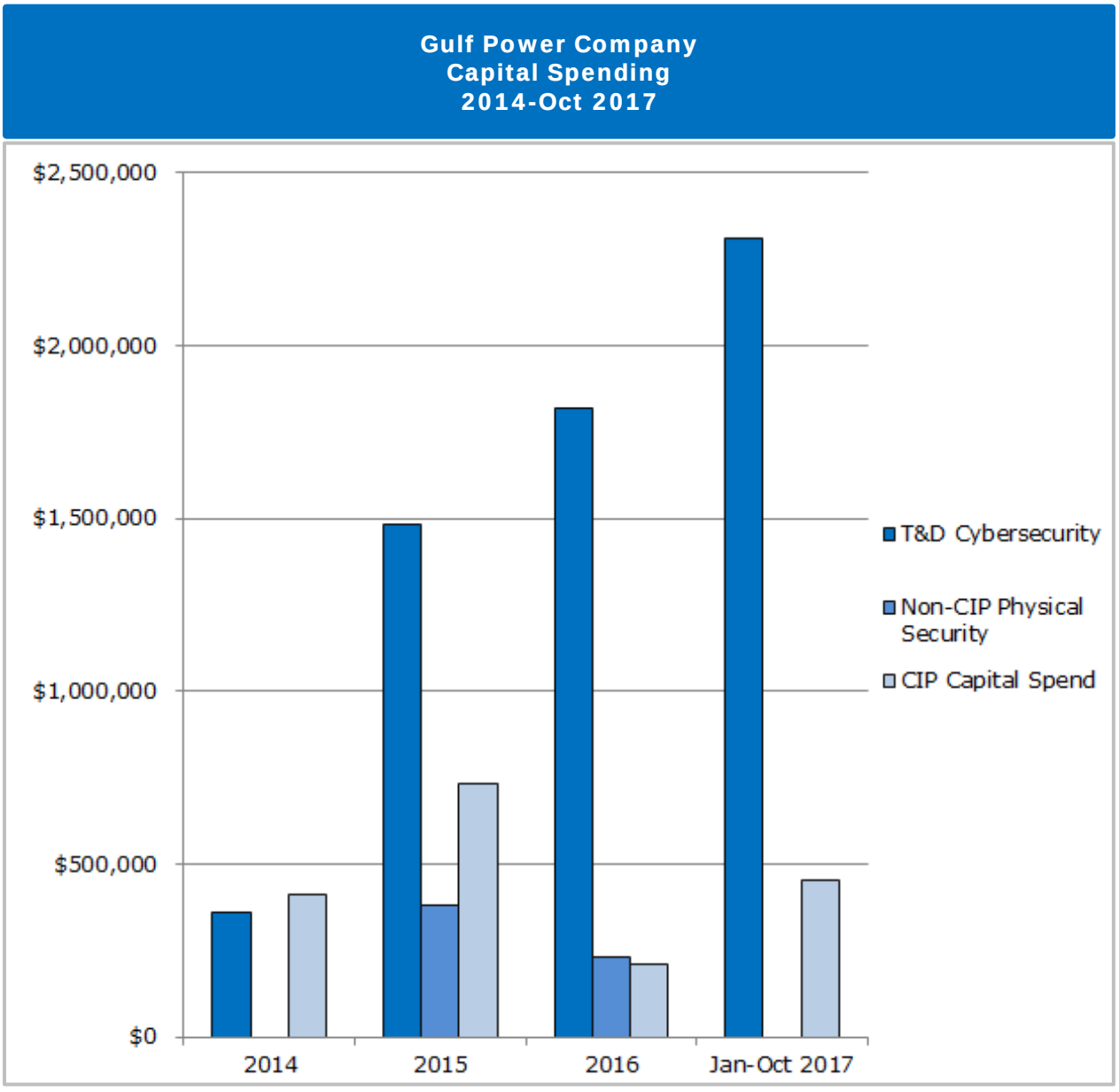


Exhibit 6 *Source: Document Request Response 2*

As Gulf implements initiatives from the Transmission and Distribution Cybersecurity Program, its cybersecurity capital spending increases each year. CIP and non-CIP physical capital investment remain comparatively low, even through the implementation of CIP Version 5. Gulf reported no capital spending on non-CIP physical security from January to October 2017.

6.0 Tampa Electric Company

TECO Energy, Inc. and its subsidiaries, including Tampa Electric Company (TEC), were acquired by Emera, Inc. on July 1, 2016. TEC is now a wholly-owned subsidiary of Emera, Inc. which is headquartered in Halifax, Nova Scotia, Canada.

TEC's serves approximately 2,000 square miles with over 725,000 residential, commercial and industrial customers. Its territory includes all of Hillsborough County and parts of Polk, Pasco and Pinellas counties. The company employs nearly 4,700 MW of generating capacity, with 195 substations, including 79 transmission substations and 118 distribution substations. TEC transmission facilities are operated at 230, 138, and 69kV. TEC's three generation facilities are Bayside, Big Bend, and Polk Power Station, along with several smaller solar-generation facilities.

6.1 Organization

TEC's Compliance Program is a part of TECO Energy's and Emera's overall Corporate Compliance Program. For administrative purposes, federal rules and regulations are grouped into subject matter areas. A Subject Matter Expert in each of the areas is assigned as the Compliance Program Coordinator and is responsible and accountable for the administration of the compliance programs for that area. TEC's compliance programs manage cyber and physical security protection and implementation of NERC CIP-002 through CIP-014. **Exhibit 7** displays TEC's Federal Energy Regulatory Compliance Program responsibilities.

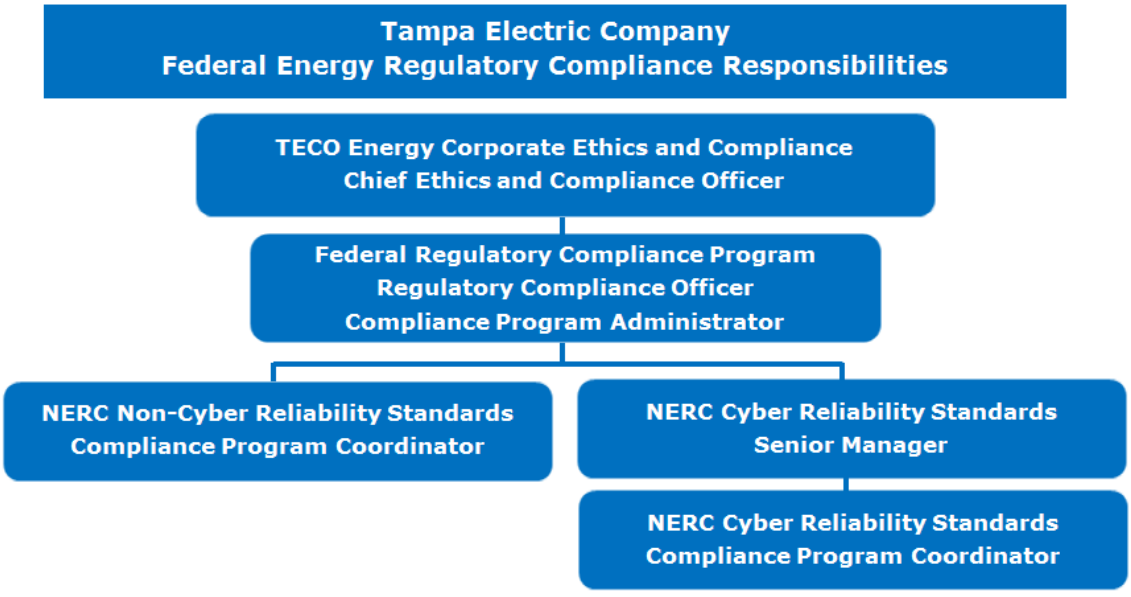


Exhibit 7

Source: Document Request Response 2.3

TEC's Federal Energy Regulatory Compliance Program is managed under the supervision and oversight of the Chief Ethics and Compliance Officer, who is responsible for ensuring effective prevention and/or detection of violations of applicable laws, regulations and ethical guidelines and to advise and recommend solutions.

6.1.1 CIP Senior Manager - Vice President of IT & CIO

NERC requires that each utility designate a CIP Senior Manager to oversee CIP compliance. According to CIP-003, Requirement 3, the CIP Senior Manager is a single senior management official. She has the overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011. For TEC, the designated CIP Senior Manager is the Vice President of Information Technology and Chief Information Officer.

6.1.2 Chief Ethics and Compliance Officer

The Chief Ethics and Compliance Officer provides supervision and oversight of the Federal Energy Regulatory Compliance Program, reviews and approves the Compliance Program document, delegates specific authority and responsibility to the Regulatory Compliance Officer, and reviews reports of regulatory compliance issues and ensure that corrective actions are taken when necessary.

6.1.3 Regulatory Compliance Officer

The Regulatory Compliance Officer delegates specific authority and responsibility to the Compliance Program Administrator and Compliance Program Coordinators, reviews, approves and follows practices and procedures for the Compliance Program and any changes to those procedures or practices. He reviews all regulatory compliance issues, reports on regulatory compliance matters at quarterly Corporate Compliance Oversight Committee meetings or directly to senior management, the CEO and the Audit Committee of the TECO Energy Board of Directors and reviews and approves the Compliance Program and procedures at least semiannually.

6.1.4 Compliance Program Administrator

The Compliance Program Administrator monitors the activities of the Compliance Program Coordinators, acts as chair of the Federal Energy Regulatory Compliance Committee, and assists each Compliance Program Coordinator in the development, implementation and proper maintenance of the necessary regulatory compliance program framework. He develops, approves and follows the administrative procedures for the Compliance Program, coordinates the company's response to compliance audits, develops periodic compliance audit activities, and serves as point of contact with regulators concerning compliance matters. The Compliance Program Administrator also reports on regulatory compliance matters at quarterly Corporate Compliance Operational Committee meetings.

6.1.5 Compliance Program Coordinators

The Compliance Program Coordinators incorporate compliance requirements of all existing and new statutory, order, rule, or regulation-based compliance obligations into the Coordinator's program area and maintain and update the Website to reflect all information relevant to the program area. They develop and implement appropriate ongoing training programs, follow the administrative procedures for the Compliance Program approved by the Regulatory Compliance

Officer, and update the Website with the designated individual or individuals to whom questions regarding the proper interpretation or application of the compliance rules and regulations can be directed on a real-time basis.

The Compliance Program Coordinator for NERC CIP is the IT Quality Assurance & Compliance Director, who is also the chair of the NERC CIP Steering Committee, whose members include the directors for all areas impacted by NERC CIP compliance. The NERC CIP Steering Committee oversees the cybersecurity protection and implementation of NERC CIP-002 through CIP-011. The Compliance Program Coordinator for NERC CIP-014 and for all the NERC Operations and Planning standards, is the Director of Tariffs, Compliance and Florida Reliability Coordinating Council Relations.

6.1.6 Policies and Procedures

TEC's cyber and physical security policy is contained within a TEC document titled *Federal Energy Regulatory Compliance Program.* This program is a part of TECO Energy's and Emera's overall Corporate Compliance Program which specifies compliance with FERC and other applicable federal agencies' rules and regulations.

The Compliance Program outlines the organization, governance, and procedures for several areas, including the NERC CIP standards. It is managed by the Chief Ethics and Compliance Officer and administered by TEC's department of Regulatory Affairs. Each of the Compliance Program Coordinators maintains a website that includes the following information pertaining to their program:

- Applicable rules and regulations
- Written procedures
- Training
- Monitoring and audits

Employees receive periodic training on applicable rules and are informed of their responsibility to adhere to the rules and regulations, including NERC reliability standards, or be subject to disciplinary action. Certain NERC CIPs specify required training for specific employees and functions.

TECO Energy's *Administrative Policy 1.12 - Information Security*, defines the cybersecurity policy for TEC and represents management's commitment and ability to secure its Bulk Electric System (BES) Cyber Systems/Cyber Assets and other devices as outlined in the NERC CIP Standards and Requirements. The cybersecurity policy also references physical security from a governance perspective.

TEC's cybersecurity policy objective is to protect the assets, integrity, and copyrighted material of TECO Energy and its subsidiaries, and to communicate the proper use of such information. All information obtained, created, developed or assembled in the performance of a TEC team member's work or using TEC's equipment or resources is considered a corporate asset. As such, it is protected from deliberate or accidental alteration and inappropriate disclosure.

TEC is required to follow NERC Emergency Preparedness and Operations and Transmission Planning standards summarized in Chapter 2 of this report. TEC Compliance Program Coordinators retain all compliance documents on the TEC Website, and other areas where related documents are stored, for the retention period specified in the *TEC Records Retention Policy for Compliance with NERC Reliability Standards.*

Through the corporate Emergency Management and Business Continuity program, the company implemented the *Cyber Security Incident Response Plan* which would be implemented for any major cyber or physical security incident. The plan identifies and classifies cybersecurity incidents, personnel roles and responsibilities, and discusses the response and notification framework for reportable cybersecurity incidents. The cybersecurity response plan contains response and notification flowcharts, Incident Command System organization structures, and checklists to help focus emergency response activities.

For compliance with new or modified NERC reliability standards, Compliance Program Coordinators and applicable Subject Matter Experts follow TEC's *NERC Compliance Plan and Internal Controls Process* shown below, which outlines a step-by-step process for developing and maintaining a compliance plan for each NERC reliability standard applicable to TEC. Each compliance plan includes the necessary steps to become and remain compliant and applicable internal controls. **Exhibit 8** displays TEC's Compliance Plan Process.

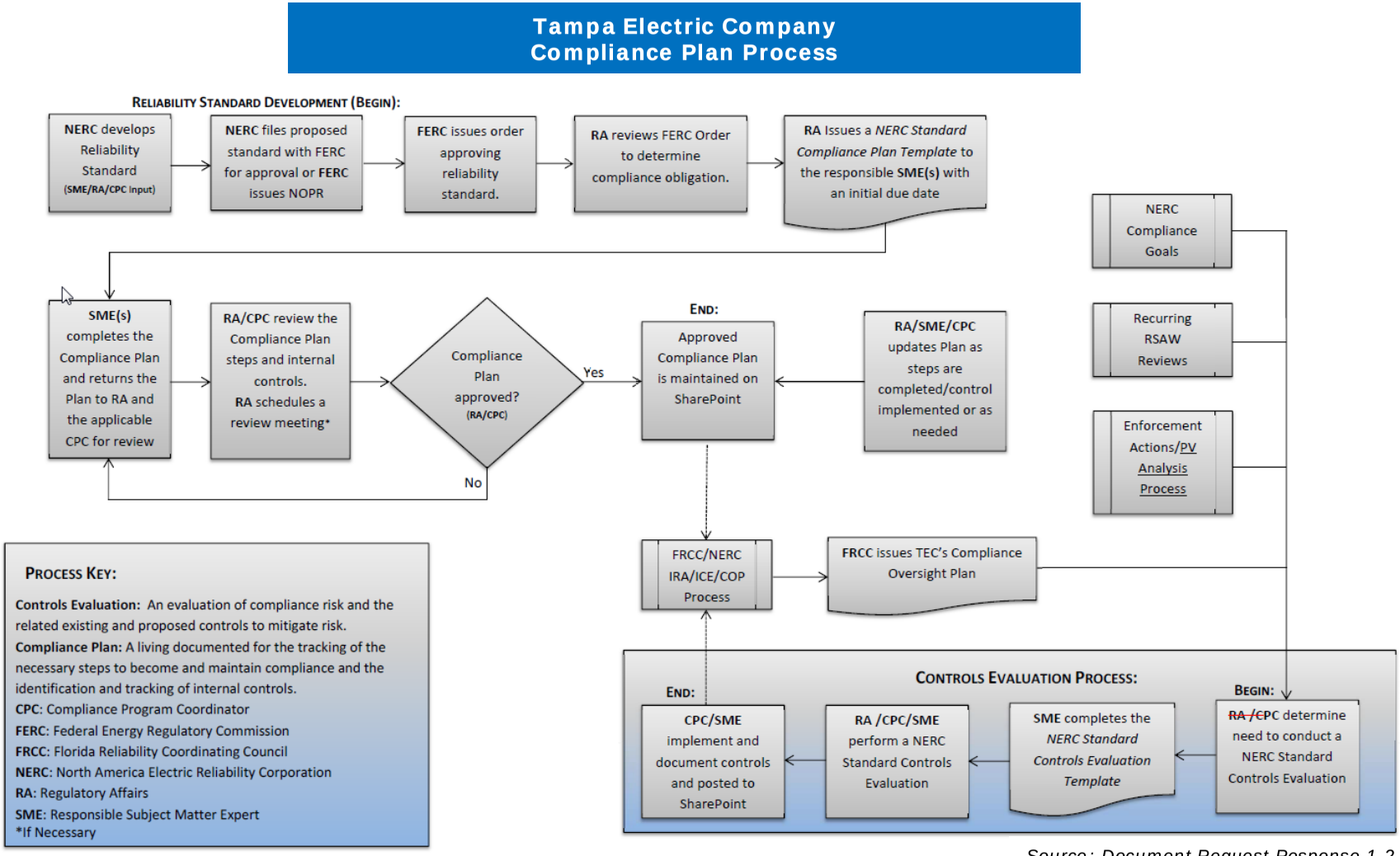


Exhibit 8

Source: Document Request Response 1.2

6.2 Cybersecurity Protections

6.2.1 Transmission Facility Protections

TEC maintains a total of 79 transmission substations, 30 of which are considered BES transmission substations. TEC states it is committed to securing its BES cyber systems, BES cyber assets, and other NERC-related devices pursuant to the NERC CIP-002 through CIP-011 Standards. TEC maintains that it interprets and applies the NERC standards, as technically feasible, in a financially responsible and operationally safe manner. TEC believes it complies in each area that corresponds with the functional entities for which it is registered with NERC's functional model as a Balancing Authority, Planning Authority/Coordinator, Transmission Operator, Transmission Operator, Transmission Owner, Generation Operator, Generation Owner, Transmission Service Provider, Resource Planner, and Distribution Provider.

According to TEC, it complies with the latest version of the NERC CIP Reliability Standards that are currently in effect as set forth in NERC's implementation plans. In accordance with NERC's implementation schedule, TEC completed its compliance plan for Version 5 requirements that were due on July 1, 2016, and the Low Impact requirements that were due on April 1, 2017.

As required by CIP-002, TEC has systematically evaluated each of its BES cyber assets or BES cyber systems to determine which are High, Medium, and Low Impact BES cyber systems per CIP specifications. NERC's categorization process is designed to identify BES cyber assets or BES cyber systems that, if compromised, would have an immediate (within 15 minutes), real-time impact on a BES Reliability Operating Service.

Following its categorization of assets, TEC implemented security management controls for High and Medium Impact BES Cyber Systems in accordance with CIP standards. TEC implemented a truncated set of security management controls for its Low Impact BES Cyber Systems by obtaining CIP Senior Manager approval for documented cybersecurity policies. These collectively address cybersecurity awareness, physical security controls, and electronic access controls for Low Impact systems and cybersecurity incident response. Under TEC's *Cybersecurity Implementation Plan*, requirements for protection of Low Impact BES Cyber Systems implementation are progressing toward the deadline of September 1, 2018.

In its compliance efforts for CIP-003, TEC implemented system security management requirements for High and Medium Impact BES Cyber Systems through programs which cover ports and services, security patch management, malicious code prevention, security event monitoring, and system access control. TEC implements its Information Protection Program to ensure that High and Medium Impact BES Cyber System Information is identified, protected, and securely handled. All information that meets the definition of BES cyber system information, whether in physical or electronic format, including electronic storage locations, is within scope of the Information Protection Program.

TEC uses the same documented methods and programs to protect BES cyber system information for Low Impact BES Cyber Systems. It implemented methods to protect BES cyber system

information for the Energy Management System that controls both transmission and distribution substations.

CIP Personnel and Training Program

TEC seeks to ensure compliance with NERC Personnel Risk Assessments by implementing and maintaining processes for personnel having actual authorized cyber access or authorized unescorted physical access to NERC CIP covered cyber assets. TEC addresses identity confirmation and requires a government-issued photo identification to establish identity for all employees and nonemployees that will require NERC access. Identity verification is also run through Social Security Number Validation in the background check.

To meet the requirements of CIP-004, TEC documents, implements, and maintains a formal NERC CIP Training Program. The complexity of CIPs and the frequent revisions to them make frequent reinforcement training necessary. TEC implemented and maintains a Security Awareness Program to ensure personnel having physical access to key assets receive on-going reinforcement in security practices at least quarterly. TEC documents the direct communications of emails, indirect communication via posters and the Intranet, management support and reinforcement activities.

TEC developed training courses for employees and non-employees, including vendors. Both courses include training on cybersecurity policies, physical access controls, handling BES cyber system information, and cybersecurity incident identification. The employee course also includes information on responding to cybersecurity incidents. TEC implements training via a Learning Management System which automatically captures the date and successful completion of the online training by an individual.

TEC employs similar training for protection of Low Impact BES Cyber Systems. To protect substation assets containing Low Impact BES Cyber Systems, TEC relies on its CIP-004 annual training to provide additional security awareness requirements. For protecting generation assets containing Low Impact BES Cyber Systems, TEC includes cyber and physical security awareness training with the annual safety and operations training.

TEC implemented similar safeguards for distribution cyber systems. Since personnel who work on distribution substation BES cyber systems also work on transmission substations systems, the processes listed above are employed.

Electronic Access

In accordance with CIP-005, TEC manages electronic access to BES cyber systems by specifying a controlled Electronic Security Perimeter in support of protecting BES cyber systems against compromise that could lead to misoperation or instability in the BES.

TEC implemented the electronic security perimeter requirements of CIP-005 for High and Medium Impact BES Cyber Systems by performing a walkthrough and verification process to ensure all cyber assets that utilize a routable protocol reside within a defined Electronic Security Perimeter and that all External Routable Connectivity negotiates an Electronic Access Point. This process results in the documentation of physical and logical network diagrams for the relevant locations.

CIP-003 Version 6, issued on January 21, 2016, requires Electronic Access Controls for Low Impact BES Cyber Systems to be fully implemented by September 1, 2018. During implementation of TEC's September 1, 2018 Low Impact Cyber Security Plan, it will evaluate and adjust the implementation plan and schedule depending on results of the physical security walkthroughs.

TEC validates the access control lists or firewall rules that deny access by default on identified Electronic Access Points. Each Electronic Access Point contains a "catch all" rule that denies access by default. Every Access Control List or firewall rule is validated to ensure sufficient justification is provided. TEC's policy is to avoid Dial-up Connectivity. TEC has implemented network Intrusion Detection System monitoring to assist in the detection of known or suspected malicious communications that cross identified Electronic Access Points. Additional controls further assist in the detection of malicious communications to prevent computers from being hijacked and controlled by hackers.

For Low Impact BES Cyber Systems, TEC has documented the high-level plan for implementing Electronic Access Controls. TEC has also implemented firewalls and access control lists safeguards for distribution cyber systems.

System Security Management

In accordance with CIP-007, TEC has implemented system security management controls for High and Medium Impact BES Cyber Systems and distribution cyber systems. The TEC Security Management System is designed to:

- Reduce the attack surface of its cyber systems by disabling any ports and services that are not needed for its applications.

- Eliminate known security vulnerabilities by evaluating security-related software patches for applicability within 35 days of release by the relevant patching source and by applying any applicable patches within the subsequent 35-day application period; or, when patches cannot be applied within the 35-day period due to system limitations, by implementing alternative means to mitigate security vulnerabilities until the patches can be applied.

- Deploy antivirus or alternate methods to deter, detect, or prevent the introduction, exposure, and propagation of malicious code on all applicable BES cyber systems/assets.

- Employ security information and event management software to monitor its BES cyber systems/assets for signs of malicious activity and to provide information for forensic analysis if malicious activity is detected. Security information and event management tools monitor and log all access into or out of any Electronic Security Perimeter and of all security events on all applicable CIP covered assets.

- Implement a suite of controls to prevent unauthorized access by cyber attackers. Where technically feasible, TEC requires authentication at the system/application level for all interactive user access.

TEC has implemented firewalls and access lists for system security management for assets containing Low Impact BES Cyber Systems and account management safeguards like removing factory default passwords. Although not required by NERC CIP standards, the company's system security practices for its Low Impact power plant cyber systems follow similar processes for patching and malware prevention to the extent allowable by vendor technology.

Change Management and Vulnerability Assessments

To adhere to the obligations of CIP-010, TEC performs vulnerability assessments for High and Medium Impact BES Cyber Systems Assets which must undergo regular cyber vulnerability assessments. These requirements distinguish between two assessment types, Paper, and Active. Paper assessments are conducted for all Medium Impact BES Cyber Systems/Assets and their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets at least once every 15 calendar months. Active assessments are conducted for all High Impact BES Cyber Systems/Assets at least once every 36 calendar months. All new High Impact BES cyber systems/assets and their associated Electronic Access Control or Monitoring Systems and Protected Cyber Assets undergo an active assessment prior to being placed into a production environment.

TEC performs change management assessments for High and Medium Impact BES Cyber Systems by implementing and maintaining a process to identify the baseline configuration, and to track and monitor changes to the baseline for applicable NERC covered cyber assets that are part of the BES cyber systems.

TEC performs both vulnerability and change management assessments for the Energy Management System that controls both transmission and distribution substations. At the present time, CIPs do not require cyber related vulnerability and change management assessments for assets containing Low Impact BES Cyber Systems. TEC is currently conducting both physical and cybersecurity assessments related to CIP-003 criteria and plans to complete compliance activities by September 1, 2018.

Proposed NERC Standards

NERC is presently finalizing CIP-012 entitled *Cyber Security – Control Center Communication Networks*. An effective date has yet to be established. The purpose of CIP-012 is to require Responsible Entities such as TEC to implement controls to protect sensitive BES data while being transmitted over communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers, the standard applies to all High, Medium, and Low Impact levels. TEC currently implements cyber controls that will meet the proposed CIP-012 compliance when it does become effective.

To mitigate cybersecurity risks to the reliable operation of the BES, TEC is implementing security controls for supply chain risk management of BES cyber systems in accordance with proposed CIP-013. An effective date for CIP-013 has not been determined, but TEC believes this procedure may become effective sometime after the fourth quarter 2019. CIP-013 addresses FERC Order No. 829 directives for entities to implement a plan that includes processes for mitigating cybersecurity risks in the supply chain. The plan is required to address the following four objectives:

- Software integrity and authenticity;
- Vendor remote access;
- Information system planning; and
- Vendor risk management and procurement controls.

6.2.2 Distribution Facility Protections

Since 2014, TEC has implemented several safeguards for distribution cyber systems, some were triggered by compliance actions in response to CIP-014. TEC's primary Distribution Control Center shares the same building and the same protections against physical attacks as TEC's primary Transmission Control Center. TEC documents the processes, tools and procedures to monitor physical access to the perimeters, and operates a Central Monitoring Station to perform monitoring activities and responses to alarms on a 24/7 basis. If an alarm cannot be successfully resolved, local law enforcement is contacted as appropriate to the circumstances.

Outages at distribution facilities or distribution cyber systems are not likely to cause widespread cascading or instability. Therefore, distribution facilities are much less attractive targets and less likely to be attacked. The CIP standards are designed to safeguard BES cyber assets that, if compromised, could cause widespread disruption of the BES.

TEC addresses cyber vulnerabilities and change management during a distribution substation construction project, and performs both vulnerability and change management assessments for the Energy Management System, including operator workstations, that control both transmission and distribution substations. TEC states that regular cyber related vulnerability and cyber change management assessments for distribution cyber systems located at the substation are neither required or nor cost-effective.

TEC has implemented a number of safeguards for system security management for distribution cyber systems such as firewalls, access lists, and account management safeguards like removing factory default passwords. The Energy Management System is used for control of both transmission and distribution substations. The Energy Management System assets that control distribution substations receive essentially the same protections as those for transmission substations.

6.3 Physical Security Protections

6.3.1 Transmission Facility Protections

Most of TEC's 79 transmission substations in the company's grid are at the 69 kV level. One new 230 kV transmission substation was installed in 2016 (Aspen), and one 69 kV transmission substation was installed in 2017 (Big Bend Solar).

In accordance with CIP-006, TEC implemented physical security protection for High and Medium Impact BES Cyber Systems by defining operational or procedural controls to restrict physical access. The Corporate Security Department and the Facility Services Department are responsible for ensuring that defined boundaries exist for High and Medium Impact NERC cyber

systems and assets, and required physical security measures are installed at each location. These measures may include firewalls, authentication servers, log monitoring, and alerting systems.

For primary and backup control centers which contain the High Impact BES Cyber Systems, Electronic Access Control or Monitoring Systems and Protected Cyber Assets, Corporate Security requires a PIN keypad and badge reader. CIP-006 requires two or more different physical access controls to allow unescorted physical access into Physical Security Perimeters to authorized individuals.

TEC utilizes an access control system to record all transactions of card key swipes and logs to uniquely identify individuals per access point 24/7. Visitor access to physically protected areas is managed by authorized business unit personnel. Visitors and contractors are required to wear identification badges and must be escorted by authorized employees when entering Physical Security Perimeters. Manual logging is used at all physically protected areas for escorted visitor access.

In response to Hurricane Irma, TEC declared a NERC CIP Exceptional Circumstance beginning on September 9, 2017, which concluded on September 25, 2017. Card key access to NERC Physical Security Perimeters was temporarily granted to four team members as part of the restoration efforts. At the conclusion of the NERC CIP Exceptional Circumstance, the card key access was removed for those four team members.

As of July 1, 2016, TEC completed efforts regarding the physical security protection requirements for CIP-006 for High and Medium Impact BES Cyber Systems by defining operational or procedural controls to restrict physical access. TEC also uses roving security guards, various forms of fencing based on risk, and card key access via security gates at facilities which house Low Impact BES Cyber Systems with bi-directional routable communication.

To identify and protect transmission stations and transmission substations, and their associated primary control centers, which, if rendered inoperable, could result in widespread instability and related issues, TEC first identified its facilities that are subject to NERC standard CIP-014. The company applied the specified criteria of a 500 kV substation, or a 200-499 kV substation that is connected to three or more other substations 200 kV or higher. Transmission studies were reviewed and approved by a qualified independent third party as required. According to TEC, it is currently in compliance with the latest version of the CIP-014 Reliability Standard, and expects all the CIP-014 Reliability Standard security measures to be completed by the end of year 2018. Company-wide expected costs to fully implement CIP-014 are estimated at over $6.5 million.

TEC's Cybersecurity Implementation Plan for assets containing Low Impact BES Cyber Systems is in progress and TEC plans to meet the implementation deadline of September 1, 2018. For distribution cyber systems, TEC has implemented firewalls and access control list safeguards.

6.3.2 Distribution Facility Protections

There are 118 TEC distribution substations with the most recent being placed in service in 2016 (J.D. Page). TEC plans to install cardkey access to the substation control houses in all substations containing Low Impact BES Cyber Systems that have bidirectional routable communication. The planned card key access will protect both the asset and the Low Impact Electronic Access Point. TEC maintains fences, gates, lighting, and physical key access for physical security control of distribution substations.

Since distribution substations generally do not contain critical BES cyber assets or BES cyber systems, TEC does not apply the High, Medium, and Low Impact BES Cyber Systems categorization process to distribution cyber assets. Unlike transmission counterparts, loss of distribution substation functions can be fairly easily alleviated with system redundancy.

6.4 Collaborative Resources

6.4.1 Industry Groups and Government Agencies

TEC networks with local, state, federal and tribal law enforcement agencies, including Fusion Centers, and Communication Centers. These interactions help maintain open communication channels if agencies have information to share.

NERC Electricity Information Sharing and Analysis Center (E-ISAC)

The E-ISAC is operated by NERC and functions as an independent group organizationally separate from NERC's enforcement processes. The E-ISAC gathers and analyzes security data, shares appropriate data with stakeholders, coordinates incident management, and communicates mitigation strategies with stakeholders. TEC monitors NERC E-ISAC resources for updated information about potential threats to the BES. E-ISAC exercises, meetings, phone conferences and webinars are attended by TEC personnel throughout the year.

NERC Critical Infrastructure Protection Committee (CIPC)

TEC takes part in the NERC Critical Infrastructure Protection Committee quarterly meetings which include presentations from the DOE, FERC, Edison Electric Institute, the NERC Electric Reliability Organization, and the E-ISAC. TEC also participates in the monthly FRCC Critical Infrastructure Protection Subcommittee meetings. These meetings include a monthly discussion of E-ISAC physical security briefings and frequently include presentations from the DHS on physical security protection. TEC's Information Technology department also participates on the monthly Edison Electric Institute Security Workgroup conference calls to discuss items of interest to both physical and cybersecurity.

Local, State, and Federal Law Enforcement

TEC personnel continuously network with local, state, federal and tribal law enforcement agencies, including Fusion Centers, and Communication Centers. The Fusion and Communication Centers include the Central Florida Intelligence Exchange and the National Infrastructure Coordinating Center – Homeland Security Information Network Critical Infrastructure. These interactions help maintain open communication channels from numerous sources of security information. State and local emergency operation centers hold exercises as

well, and TEC participates in biennial NERC GridEx Exercises which include participants from other states, Mexico, and Canada.

TEC also participates in annual storm exercises held by the cities and counties where electric service is provided by TEC, including Hillsborough, Pasco, Pinellas, and Polk Counties, as well as the City of Tampa. In 2015, Hillsborough County and City of Tampa Emergency Operation Centers participated in the NERC GridEx III cybersecurity exercise with TEC.

United States Coast Guard (USCG)

TEC took part in Coast Guard Exercises which incorporated debris cleaning, cybersecurity, active shooter, hurricane, and maritime security exercises in 2015, 2016, and 2017. TEC participates in annual USCG Maritime Security drills and exercises. The Maritime Security drills reflect the prevailing threat environment to marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

Electric Power Research Institute (EPRI)

TEC continues to monitor a joint initiative to develop technical bases by which electric companies can address Electromagnetic Pulse (EMP) threats. The joint initiative is described in the January 2017 report, *U.S. Department of Energy Electromagnetic Pulse Resilience Plan* which outlines a joint strategy developed by the DOE and the EPRI with research conducted by the Department of Defense, Idaho National Laboratory, and other national laboratories. The report's action plan includes eight elements:

- Generate a shared understanding of potential EMP effects
- Identify gaps in EMP knowledge
- Coordinate government-industry information sharing
- Develop unclassified composite E1/E2/E3 waveforms for use by industry in modeling/testing their systems
- Provide an understanding of the susceptibility of specific critical electric grid components to EMP waveforms
- Evaluate interactive EMP system and component modeling capabilities
- Develop realistic risk-based EMP planning scenarios for use by industry for planning purposes and assess/model expected damage for each scenario
- Report on potential issues of concern for critical infrastructure from the loss of off-site utility power from EMP

The report acknowledges that certain activities will require coordination between DHS, NERC, FERC, the Department of Defense, the Federal Emergency Management Agency, State officials, and industry.

Edison Electric Institute (EEI)

TEC participates in the Edison Electric Institute Spare Transformer Equipment Program (STEP), an electric industry program that strengthens the sector's ability to restore the nation's transmission system more quickly in the event of a physical attack. STEP represents a coordinated approach to increasing the electric power industry's inventory of spare transformers

and streamlining the process of transferring those transformers to affected companies in the event of a transmission outage caused by a terrorist attack. Under the program, each participating energy company is required to maintain and, if necessary, acquire a specific number of transformers. STEP requires each participating company to sell its spare transformers to any other participating company that suffers a triggering event, defined as an act of terrorism that destroys or disables one or more substations and results in the declared state of emergency by the President of the United States.

Department of Energy (DOE)

If a physical security incident or cybersecurity incident disrupts or attempts to disrupt the operation of a BES System, it is reported to the E-ISAC by the TEC Physical Security Director within one hour of determination, and communicated to the TEC NERC Representative. If the incident causes major interruptions or impacts to critical infrastructure facilities or to operations, or is a cyber event that causes interruptions of electrical system operations, the incident must be reported to the DOE by means of DOE Form OE-417. This Electric Emergency Incident and Disturbance Report collects information on electric incidents and emergencies. The DOE uses the information to fulfill its overall national security and other energy emergency management responsibilities, as well as for analytical purposes.

Department of Homeland Security (DHS)

The DHS works closely with the DOE and the electric sector to ensure the security, resilience, and reliability of the U.S. power grid. TEC has conducted the Cybersecurity Evaluation Tool (CSET), Cybersecurity Capability Maturity Model (C2M2) and security controls reviews with the DHS and Federal Bureau of Investigation. The Cybersecurity Evaluation Tool is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate their industrial control system and information technology network security practices. The C2M2 was developed by a public-private partnership effort established to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid. It is a voluntary self-evaluation process utilizing industry-accepted cybersecurity practices to measure the maturity of an organization's cybersecurity capabilities. It is designed to measure both the sophistication and sustainment of a cybersecurity program. TEC performs risk assessments for each of its critical facilities, and uses the same Homeland Security threat levels.

6.4.2 Exercises and Assessments

Grid Ex Simulated Exercise

Since 2011, NERC sponsored biennial internationally distributed physical and cybersecurity exercises within US, Canada and Mexico. GridEx is focused on testing physical and cybersecurity plans in the areas of preparedness, mitigation, protection, response and recovery.

TEC participated as an active participant within the GridEx Working Group which develops the scenarios and all the documents used in the exercise. During GridEx's off-years, TEC conducts internal exercises to further test plans and document plan improvements.

Exhibit 9 shows physical and cybersecurity exercises in which TEC participated as an active participant since 2011.

Tampa Electric Company Physical and Cybersecurity Exercises 2011-2019		
Year	**Exercise Name**	**Date(s)**
2011	GridEx I*	November 16-17, 2011
2012	Phish Hook/ Bugsplat Annual Cyber Exercise	November 9, 29, 30, 2012
2013	GridEx II*	November 13-14, 2013
2014	Annual CIP-008 & Privacy Breach Exercise	November 19, 2014
2015	GridEx III*	November 18-19, 2015
2016	Ransomware Attack*	April 7, 2016
2017	CIP-003 R2 - Low Impact Facilities	March 20, 2017
2017	HMI Attack - Medium & High Impact	June 26, 2017
2017	GridEx IV*	November 15-16, 2017
2018	Annual CIP-008 Exercise	TBD
2019	GridEx V*	TBD

*Also satisfies the CIP-008 annual requirement.

Exhibit 9 *Source: Document Request Response 1.22*

Self-Initiated Protection Measures

TEC's self-initiated actions to protect against physical security threats are based on multi-layered security actions that consist of five layers: Deter, Detect, Deny, Delay, and Defend. TEC's physical asset controls include:

- Fences and locked gates
- Electronic lock control mechanisms
- Card keys and card key readers
- Security guards
- Armed security response
- Crash-proof gates
- Pulse-type power on some fences and gates
- Concrete security barricades
- Radar intrusion detectors on some sites
- Anti-ballistic barriers
- Remotely Controlled Active Defense and Denial Systems
- Enhanced access control
- 24-hour watch by the Central Monitoring Station and the Security Operation Center

TEC partners with local, county, state, and federal law enforcement and can draw upon additional law enforcement resources depending upon the size and jurisdiction of the potential threat.

Self-Initiated Cybersecurity Protection Measures

Aside from CIP Reliability standards, TEC has self-initiated a number of actions to protect against cybersecurity threats. For example, TEC performs Internal Control Evaluations as part of the ongoing NERC CIP Compliance efforts. TEC engaged third-party security firms to perform

security assessments on key systems (e.g., Smart Grid Communications and voltage and reactive power control system, Radio Frequency, Energy Management System (EMS), Patch Management, Public Key Infrastructure, etc.) to ensure TEC exercises due care and due diligence. As a result of the studies and assessments, the company enhanced physical security surrounding cyber assets by adding multiple layers of physical and electronic security barriers which make cyber assets a harder target.

TEC states that it conducts periodic unannounced phishing simulations to test its susceptibility to infiltrations/hack attacks. The phishing simulations typically go to all TECO Energy employees, but on some occasions phishing simulations have been sent to specific groups where there were higher click rates. TEC also conducts vulnerability assessment scans on a regular basis for all internal and Internet-facing network environments that can be accessed via routable protocols. Scans for rogue wireless access points at NERC Physical Security Perimeters are also conducted on a periodic basis.

6.4.3 Audits

Each year, TECO Energy's Director of Audit Services reviews the company's annual strategy plan and discusses trending risks and significant upcoming initiatives with all middle and senior management. The Information Security Director provides perspective on IT challenges or concerns surrounding major activities such as cybersecurity, safeguarding data, and vendor management. The Director of Audit Services develops each year's internal Audit Plan through discussions with financial, regulatory, and operational management.

In 2016, TECO Energy's Audit Services was requested to facilitate a patch management assessment specific to the Corporate IT environment. The assessment was performed to gain an understanding of the challenges the organization faces under its current processes, advise on the development of an improved process that includes risk analysis and mitigation strategies, and identify opportunities for enhanced efficiencies through automation and process optimization. Audit Services engaged an external cyber risk management company to perform the assessment. The assessment identified risk factors and challenges such as accuracy of patch exceptions, and improving communication of new servers. Audit Services and the third-party cyber risk management company suggested process changes which management agreed to incorporate.

In 2017, TECO Energy's Audit Services conducted an upgrade control review of its EMS. The project included upgrading the EMS application, the Operating System software and the related server hardware. The EMS monitors, controls and optimizes the performance of the generation, transmission and distribution assets for TEC. The EMS application is subject to the NERC CIP standards. Audit Services worked with management to identify and rank project risks and to assess the proposed system control design. Audit Services identified system control risks associated with system availability, system access and regulatory compliance. Proposed controls were determined to be designed appropriately prior to placing the system in service. The EMS Upgrade went into service in June 2017.

A joint FRCC and NERC audit of the TEC's main control rooms and transmission substations was conducted in 2017, including onsite inspections and interviews. TEC planned and outlined responses to any outstanding compliance issues raised by auditors. Also in 2017, the FRCC

conducted a recertification of the Balancing Authority/Transmission Operator functionality, and audited the backup control center as part of the FRCC Operations and Planning Audit.

6.5 Incident Reporting, Response, and Recovery

6.5.1 Reporting and Response Planning

NERC defines a cybersecurity incident as any malicious or suspicious event that compromises or is an attempt to compromise, an electronic or physical security perimeter, or disrupts, or was an attempt to disrupt, the operation of a BES cyber system. The implementation of a cybersecurity incident response plan minimizes the risk to the reliable operation of the BES caused as the result of a cybersecurity incident and provides feedback for improving the security controls applying to BES cyber systems. CIP-008 obligates entities to follow a written "*Cyber Security Incident Response Plan*" when an incident occurs or when conducting testing. It ensures the plan represents the actual response and does not exist for documentation only. NERC Emergency Operations Planning EOP-004 requires the reporting of events which include disturbances or unusual occurrences that jeopardize the operation of the BES, or result in system equipment damage or customer interruptions.

TEC developed and implemented a *Cyber Security Incident Response Plan* to identify, classify, and respond to cybersecurity incidents. TEC's *Cyber Security Incident Response Plan* applies to Low, Medium, and High Impact BES Cyber Systems along with distribution cyber systems. The plan identifies and classifies cybersecurity incidents, personnel roles and responsibilities and defines the response and notification framework for reportable cybersecurity incidents. The cybersecurity response plan contains response and notification flowcharts, Incident Command System organization structures, and checklists to help focus emergency response activities.

The DOE requires reporting for electric emergency incidents and disruptions in the United States on its form DOE-OE-417. The company must provide a description of the incident on the form and actions taken to resolve it, and if possible, the cause of the incident or disturbance, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. TEC experienced no reportable security incidents that would require submittal of a DOE-OE-417 form during the period of 2014 through April 2018.

6.5.2 Recovery Planning

NERC CIP-009 requires recovery plans are put in place for critical cyber assets and that these plans follow established business continuity and disaster recovery techniques and practices. According to TEC, it maintains multiple recovery plans for High Impact and Medium Impact BES Cyber Systems, associated Electronic Access Control or Monitoring Systems of the Electronic Security Perimeters, and Cyber Assets that authorize and/or log access to the Physical Security Perimeter Access Control Systems. BES Cyber Systems are mapped to Recovery Plans via the CIP-002 categorization processes. Each plan is mapped to its associated High Impact BES Cyber Systems, the Medium Impact BES Cyber Systems, and the associated Electronic Access Control or Monitoring Systems and Physical Access Control Systems.

Although Low Impact cyber system recovery is not addressed in CIP-009 requirements, TEC's assets containing Low Impact BES Cyber Systems are included in its *Cybersecurity Implementation Plan.* TEC believes it will complete implementation by September 1, 2018. The same recovery plan is used for all substation cyber systems including those at distribution substations.

NERC implemented EOP-005 to ensure plans, facilities, and personnel are prepared to enable system restoration from blackstart resources of an electric power station or a part of an electric grid without relying on the external electric power transmission network. The purpose of EOP-005 is to ensure reliability is maintained during restoration and priority is placed on restoring the interconnection.

In accordance with EOP-008, TEC retains a plan to continue reliability operations in the event its main control center becomes inoperable. TEC maintains interim and backup control centers in the event TEC's main control center is not operational.

NERC EOP-011 adopts FERC directives in Order No. 693 related to emergency operations and planning. It addresses the effects of operating emergencies by ensuring each transmission operator and balancing authority such as TEC develop an operating plan to mitigate operating emergencies, and coordinate with the FRCC. The FRCC, the Reliability Coordinator for the FRCC Region, has the highest level of authority, and is responsible for the Reliable Operation of the Bulk Electric System. Therefore, FRCC has the responsibility and authority to act and to direct system operators anywhere in the region to take whatever steps are necessary to maintain or restore the Reliable Operation of the Bulk Electric System.

TEC considers security and restoration plans, disaster recovery plans, and incident response plans as Critical Energy Infrastructure Information which it retains as confidential information. FERC defines Critical Energy Infrastructure Information as specific engineering, vulnerability, or detailed design information about physical or virtual critical infrastructure that:

- Relates details about the production, generation, transmission, or distribution of energy;
- Could be useful to a person planning an attack on critical infrastructure;
- Is exempt from mandatory disclosure under the Freedom of Information Act; and
- Gives strategic information beyond the location of the critical infrastructure.

TEC Emergency Management Program Command Structure

TEC assigns specific roles and responsibilities to employees responsible for recovering or re-establishing NERC-protected assets. The company designates who shall communicate with outside agencies, such as NERC, FERC, and law enforcement in the event of an emergency or cybersecurity incident. TEC follows a NERC Emergency Notification Tree to complete notifications in compliance with reporting times. Should a major cyber or physical attack occur, the TEC Regulatory Officer would notify and update the Florida Public Service Commission, and TEC's Emergency and Business Continuity Director would notify the Florida Department of Emergency Management. If the Florida Department of Emergency Management activates the State Emergency Operations Center, then communications will continue through the TEC State Emergency Operations Center Liaison. **Exhibit 10** shows TEC's Emergency Management

Program Command Structure which includes an Incident Commander (who can be either the TEC President or the TECO Services, Inc. President), Command Staff made up of the Public Information Officer, Liaison Officer, and Safety Officer, with Section Chiefs for Operations, Planning, Logistics, and Finance/Administration.

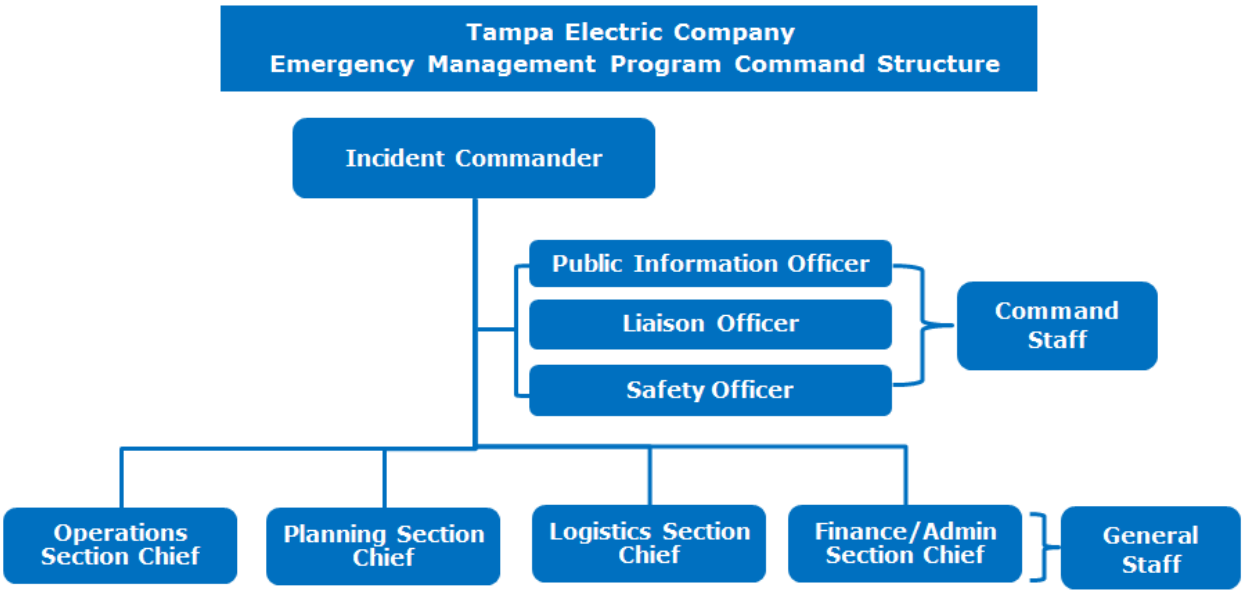


Exhibit 10

Sources: Document Response 2.3 & DR 4.3

The Director of Corporate Security and Emergency Management briefs the President of TECO Services, Inc. immediately regarding any current physical or cybersecurity threats or recent incidents that have impacted TEC. The President of TECO Services, Inc. decides whether any information provided in a briefing merits further communication to the board. These briefings occur as required, however, no recent elevated physical or cyber threat levels or physical or cybersecurity incidents have required reporting to the board.

6.6 Cyber and Physical Security Cost Tracking

TEC tracks the costs of ongoing day-to-day NERC CIP compliance as well as costs of implementing NERC CIP standards revisions and/or new standards using separate cost centers and associated project schedules. This includes IT internal labor, materials & supplies, hardware & software maintenance and acquisitions, external labor and any other associated costs.

Non-NERC ongoing cyber security costs are tracked through the cyber security department cost center. Maintenance costs for cyber security are tracked via the IT maintenance cost center and supporting spreadsheets. Generally, cyber security capital projects are tracked at a project level with separate funding project numbers.

TEC states that its corporate physical security department 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. Costs can not be separated to show the total costs of physical security alone.