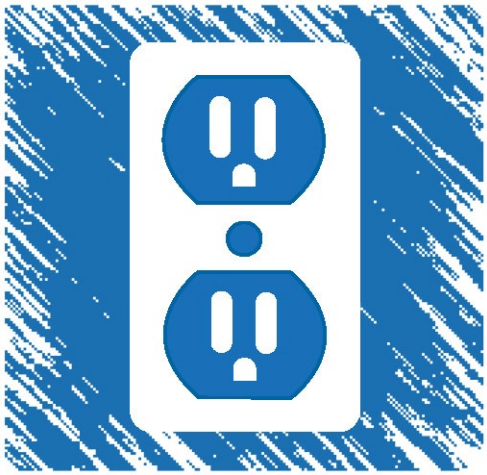

Review of

Cyber and Physical Security Protections

Florida Power & Light Company

February 2023

BY AUTHORITY OF

The Florida Public Service Commission
Office of Auditing and Performance Analysis

Review of

Cyber and Physical Security Protections

Florida Power & Light Company

Carl Vinson
Public Utilities Supervisor
Project Manager

Jerry Hallenstein
Senior Analyst

Vic Cordiano
Public Utility Analyst IV

Matthew Sibley
Public Utility Analyst IV

February 2023

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

PA-22-01-001

TABLE OF CONTENTS

TABLE OF EXHIBITS

1.0 Executive Summary

This audit report addresses cybersecurity protections employed by Florida Power & Light Company (FPL) over the period 2019-2022, including the status of protections for Gulf Power Company's systems and controls integrated since the acquisition of Gulf by NextEra Energy (NEE) in 2019.

1.1 Scope and Objectives

The primary objectives of this audit were to review, evaluate, and document the following:

- Results of recent North American Electric Reliability Corporation (NERC) compliance audits, company internal audits, and external reviews assessing compliance with NERC Critical Infrastructure Protection (CIP) reliability standards
- Self-evaluation efforts and external/internal audit activities to enhance cyber and physical security protections and planning
- Approach to risk management through compliance monitoring and internal control activities
- Implementation of self-initiated cybersecurity internal controls and compliance practices
- Cyber and physical security incident reporting internal controls as required by NERC, Department of Energy (DOE), and the Florida Public Service Commission (FPSC or Commission)
- Coordinating protections for Information Technology (IT) and Industrial Control Systems (ICS)/Operational Technology (OT) systems and proactively identifying and mitigating threats
- Controls to protect against compromises that exploit supply chain and/or cloud service vulnerabilities
- Processes for proactive cyber and physical security threat hunting and intrusion detection
- Realignments of work units and assignments for oversight of cyber and physical security protections
- Participation in response and recovery readiness simulations, drills, and exercises
- Enhanced sharing of cyber and physical security information between utilities, industry associations, state and federal regulatory agencies, and law enforcement

- Methods for separately tracking and identifying cyber and physical security costs and investments

- Lessons learned, plans, and preparations for reporting and recovering from cyber and physical security attacks

1.2 Audit Staff Observations

Through its review, Commission audit staff observed the following:

- Federal regulations such as NERC CIP requirements, and actions by the Department of Homeland Security (DHS), DOE, and other agencies have laid a solid foundation for protecting the most critical U.S. Bulk Electric System (BES) cyber assets operated by FPL.

- Most of FPL's assets within the FPSC's jurisdiction (i.e., below 100 kV) fall outside of existing NERC CIP reliability standards.

- Federal Energy Regulatory Commission (FERC), Southeastern Electric Reliability Corporation (SERC), and NERC compliance audits continue to be effective and valuable enforcement tools.

- Though cyber attacks, such as SolarWinds, Colonial Pipeline, Kaseya, and Log4j, have impacted industry operations worldwide, no cyber attack on the U.S. electrical grid has resulted in significant customer outages.

- FPL continues to assess the impacts of recent cyber and physical security attacks and to review process and control improvements related to system redundancies, network segmentation, interactions with third-party vendors, and other security needs.

- Revisions to NERC CIPs increasingly require selected protections previously mandated for High Impact and Medium Impact BES Cyber Assets to also be provided for Low Impact BES Cyber Assets.

- The ever-changing threat environment forces utilities to continually reassess protections and resource allocations.

- Compliance costs related to new and revised DOE, DHS, and NERC reliability standards continue to rise.

- To enhance its overall program of physical and cybersecurity protection, FPL has made extensive use of external consultant expertise, established a CIP Center of Excellence Program, and initiated a comprehensive key enterprise asset risk protection approach.

2.0 Background and Perspective

2.1 Limited FPSC Cybersecurity Protection Jurisdiction

The Commission has limited jurisdiction over cybersecurity protection for the U.S. Bulk Electric System (BES). It has jurisdiction over the distribution and smaller transmission facilities below a 100 kV rating. FERC sets rules and standards for protecting the interstate transmission grid, which presents a higher-value target for attacks and disruptions than does the distribution grid. FERC's national protection standards impose a comprehensive set of requirements designed to defend critical assets and ensure reliable operation of the BES.

2.1.1 Commission Rules and Jurisdiction

Despite the limitations noted above, several Florida statutes do assign specific powers and requirements to the Commission. 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 "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., requires 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 may 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 BES, those transmission facilities rated at or above 100 kV.

Exhibit 1 lists the existing Commission rules for construction of new transmission and distribution facilities, including records of 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 2022	
Rules	**Purpose/Description**
25-6.018, F.A.C.	***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, F.A.C.	***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, F.A.C.	***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, F.A.C.	***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, F.A.C.	***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, F.A.C.	***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, F.A.C.	***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 1 *Source: Chapter 25-6, Florida Administrative Code*

2.1.2 Prior Cybersecurity Reviews by Commission Audit Staff

In prior reviews, audit staff confirmed the need for the Commission to keep abreast of efforts taken by Florida IOUs to identify, protect, detect, respond, and recover from cyber and physical security attacks. Reports issued in 2014, 2018, and 2022 addressed protections of physical and cyber assets for Gulf Power Company, FPL, Duke Energy-Florida (DEF), and Tampa Electric Company (TEC). In February 2022, audit staff completed a follow-up review of the cybersecurity protection measures used by DEF and TEC.

Review of Physical Security Protection of Utility Substations and Control Centers (2014)

Commission audit staff's 2014 report[1] focused on how the four largest Florida IOUs' provide physical security measures protecting transmission and distribution substations and system

[1] http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf

control centers. At that time, utilities were in the process of implementing CIP-014 regarding 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. Audit staff examined each company's approach to analyzing, improving, and measuring physical security. The following key observations are noted in the 2014 report:

- 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 BES cyber assets operated by Florida IOUs.

- Most 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 costs must be weighed against potential benefits and perceived risks, cost recovery of physical security costs may become a significant issue.

Review of Cyber and Physical Security Protection of Utility Substations and Control Centers (2018)

Commission audit staff's 2018 report[2] primarily focused on the largest IOUs' compliance efforts related to the NERC's reliability standards. Audit staff examined each company's plans to comply with new or changing requirements over the period 2015 through 2017. The report included the following key observations:

- Certain NERC CIPs now require that selected protections previously mandated for only High Impact and Medium Impact BES Cyber Assets also must cover Low Impact BES Cyber Assets.

- 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[3] the BES 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] http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf

[3] According to NERC's terms and definitions, the reliable operations of the BES would be affected if a cyber asset is disrupted within 15 minutes of its required operation and it adversely impacts one or more BES facilities, systems, or equipment.

Review of Cybersecurity Protections Duke Energy Florida, LLC and Tampa Electric Company (2022)

Commission audit staff's 2022 report[4] primarily focused on DEF's and TEC's cybersecurity management oversight, compliance efforts related to the NERC's reliability standards, and current cybersecurity protection trends and issues. The report included the following key observations:

- Federal Energy Regulatory Commission (FERC), Southeastern Electric Reliability Corporation (SERC), and NERC compliance audits continue to be an effective, rigorous, and valuable enforcement tool.

- Independent of NERC CIP regulatory requirements, DEF and TEC continue to assess necessary system protections to guide decision-making regarding cyber and physical security investments.

- Continuing efforts and costs lie ahead for DEF and TEC to comply with new and revised DOE, DHS, and NERC reliability standards.

- Selecting and implementing prudent, proportionate defenses against physical and cybersecurity attacks requires continuous vigilance, frequent reassessment of changing risks, and active management prioritization of a security culture.

2.2 Convergence of Information/Operational Technologies

Electric utilities' computer systems are predominantly bifurcated into two types of networks: Information Technology (IT) and Operational Technology (OT).

IT networks include the servers, computers, and hardware that allow utilities to transmit, store, recover, and exchange data to run a utility's "business side," i.e., functions such as billing, customer service, and accounting.

Conversely, OT networks are industrial-oriented and include the hardware, software, and electronic devices used to generate, transmit, and distribute electric power on the "operations side." The hardware and software components of the OT network include the utility's ICS, such as a Supervisory Control and Data Acquisition (SCADA) system that monitors and controls plant equipment and power generation, and an Outage Management System that provides real-time control of outages and repairs.

Digitalization has accelerated IT and OT systems convergence. Through convergence, electric utilities such as FPL have streamlined processes allowing for greater efficiencies such as improved data collection for operational decision-making and real-time system degradation warnings to reduce repair time. However, without procedural or technical controls, the convergence of IT with OT increases the potential risk to cybersecurity threats and attacks. A

[4] http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/2022_DukeEnergy_TECO_Cybersecurity.pdf

successful attack on a utility's OT network has potential to negatively impact portions of the power grid.

Effective communication between IT and OT personnel and devices can mitigate the increased risk of OT compromise. FPL continues to improve its cybersecurity OT protections to manage and monitor system access, track OT assets, detect malicious activity, and isolate unwanted traffic by implementing network segmentation.

2.3 Supply Chain and Cloud Services Threats

Cybersecurity threats facing electric utilities include the cyber threats that plague other industries such as malware, viruses, worms, trojans, spyware, and ransomware. Today, advanced persistent threat actors including nation-state actors, increasingly target large firms for ransomware payoffs and/or to cause infrastructure damage and operational shutdown.

These actors increasingly target supply chain vulnerabilities to launch ransomware attacks. Utilities' necessary reliance on vendors for system software and hardware within the IT and OT environments elevates the importance of assuring the integrity of both. This chain of events may or may not involve malicious intent on the part of the vendor, who may unknowingly become a conduit for an attack. With IT and OT convergence, weak controls along the supply chain now increase the risk of a power outage through OT compromise.

In response to growing supply chain risks, FERC approved a new supply chain reliability standard, CIP-013, and revised CIP-005 and CIP-010. The CIP-013 standard and other revisions became effective on October 1, 2020. They require owners and operators of the BES to develop and implement supply chain management security controls to protect ICS hardware, software, and computing and networking services. These standards cover the following key security objectives:

- Software integrity and authenticity verifications
- Vendor remote access procedures
- Information system maps and plans
- Vendor risk management and procurement controls

A key security risk mitigation measure is the use of a Software Bill of Materials (SBOM) which describes the software components and firmware in the third-party product, whether purchased or obtained through open source. An SBOM allows the utility or supplier to identify potential risks before exposing OT and IT systems. It also allows end users to ensure that patching is up to date.

Increased focus on SBOM use will provide additional protection against malware attacks. SBOM information provided by a software vendor can serve to either retrace the origins of malware or to validate the authenticity of software and firmware components used in creating the product. Like nutritional information required in food product labelling, SBOMs give purchasers greater insight into the contents of products being consumed so that associated risks can be considered.

Although SBOM use is voluntary, NERC encourages electric utilities to use SBOMs to satisfy the NERC CIP reliability standards for improved software supply chain security and vulnerability response. Presidential executive orders and collaborative work with industry partners and government agencies also support SBOM use.

The increasing use of cloud computing services represents a growing cybersecurity risk to the electric industry. To streamline solutions and reduce the expense of owning and operating data centers, utilities are turning to third-party cloud service providers. Cloud computing provides additional computer system resources such as storage space, network bandwidth, and applications. By migrating to the cloud, utilities necessarily relinquish some cybersecurity responsibilities to a third party, requiring a need to coordinate with vendors and monitor protections in use.

2.4 Distributed Energy Resource Deployment Threats

Increasing deployment of Distributed Energy Resources (DERs) also introduces potential cybersecurity challenges for electric utilities. DERs are small, modular, energy generation and storage technologies, such as small wind turbines, rooftop solar systems, electric vehicles/ charging stations, and battery storage. They are connected to the distribution system and often installed on the customer side of the meter. These DERs typically produce less than 10 megawatts and provide grid reliability by supplying electric capacity when and where needed.

Grid-integrated DERs introduce uncertainty due to their interconnection with the company-owned distribution system. This interconnection makes the supply-demand relationships complex, requiring optimization tools to balance the network, and placing higher pressure on the transmission network. It also introduces security risks associated with the reverse power flow from the distribution system to the transmission system.

As DER deployment and aggregation of these small systems become more ubiquitous, they present a larger target of opportunity for cyber attacks aimed at system disruption. Therefore, the monitoring and managing of utility-owned or third-party DERs increase cybersecurity challenges for electric utilities, particularly in light of bidirectional power flow and IT/OT convergence.

According to a recent DOE report,[5] although a cybersecurity attack on DERs today "may have a limited, local impact on grid operations," as DER deployment increases, so does the risk of cyberattacks "with the potential for a broader impact." The DOE also recommends DER providers ensure that cybersecurity is a "core component" in their DER designs.

The rapid growth in DER deployment will continue to "have a significant impact on how registered entities plan, design, and operate the BPS."[6] This has led to utility investment in DER

[5] DOE, *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid,* https://www.energy.gov/eere/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy, October 2022.
[6]NERC, *Quick Reference Guide: Distributed Energy Resource Activities - DER Modeling Study* https://www.nerc.com/pa/Documents/DER_Quick%20Reference%20Guide.pdf, November 2022.

management system (DERMS) software platforms that provide early cyber threat detection capabilities designed to control continuous, real-time visibility and monitoring of DER impact on the distribution system. FPL is selectively implementing DERMS protections within its system operations.

2.5 Cyber and Physical Attacks and Ongoing Vulnerabilities

Recent notable cyber and physical security attacks are discussed in detail below. Each of these attacks holds implications for Florida IOUs and provides lessons learned to be considered.

Ukraine

In 2015 and 2016, the Sandworm advanced persistent threat group, which is associated with the Russian government-sponsored intelligence agency, deployed malware[7] to cause power outages in Ukraine. The 2015 attack was the first confirmed cyber attack to cause extensive customer power outages. It compromised information and control systems at three Ukrainian state-owned electrical distribution utilities. 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. In 2016, a fully-automated second cyber attack gained access to the Ukrainian utilities' networks. Sandworm used the malware to attack a transmission system control center causing a portion of Kyiv to lose power for over an hour.

More recently, in April 2022, the Computer Emergency Response Team of Ukraine (CERT-UA) reported that Sandworm targeted a high-voltage electrical substation in Ukraine using a malware known as Industroyer2. Sandworm planted the malware on systems within a regional Ukraine energy firm after apparently gaining access in February 2022. The malware can directly interact with electrical utility equipment and send commands to substation devices that control the flow of power. Sandworm moved laterally from the IT network to the ICS network. Fortunately, the cyber attack was detected and mitigated before a blackout occurred that would have impacted roughly two million people.

SolarWinds

On December 13, 2020, the most widespread supply chain malware attack to date in the U.S. was discovered. Malicious actors, directed by the Russian Foreign Intelligence Service, penetrated U.S. software developer SolarWinds, inserting malware into an update being developed for distribution to customers using SolarWinds' Orion business software. The supply chain attack allowed hackers to access the network of U.S. cybersecurity firm FireEye, which provides hardware, software, and services to investigate cybersecurity attacks and protect against malicious software. FireEye detected the supply chain breach and recognized that attackers entered through a backdoor in the SolarWinds software via an update to be distributed to customers. Once the update was sent to nearly 18,000 SolarWinds customers, the infection (since dubbed SUNBURST) rapidly spread worldwide.

[7] Cybersecurity companies ESET and Dragos named the malware "Industroyer" and "Crash Override," respectively.

Affected organizations worldwide included NATO, the U.K. and U.S. governments, the European Parliament and Microsoft. SolarWinds stated that its customers included 425 of the U.S. Fortune 500 companies, the top ten U.S. telecommunications companies, electrical utilities, the top five U.S. accounting firms, all branches of the U.S. Military, the Pentagon, the State Department, and hundreds of universities and colleges worldwide.

SolarWinds has since introduced new software development practices and technologies to strengthen its cybersecurity protections.

Colonial Pipeline

On May 7, 2021, Colonial Pipeline, a gasoline and jet fuel system serving the southeastern United States, suffered a ransomware cyber attack. According to the FBI, the attack was the work of REvil, a Russian-based hacking organization and a closely-associated ransomware group known as DarkSide. To contain the attack, Colonial quickly shut down its pipeline believing the hackers may have obtained information allowing them to damage vulnerable parts of the pipeline. While the OT systems were not affected, the company's IT billing system was compromised. This was the most successful cyber attack to date on a U.S. energy sector infrastructure target.

Colonial paid the requested ransom (75 bitcoin or $4.4 million) within several hours after the attack. The hackers sent Colonial Pipeline a software application to restore its network, which still operated very slowly. The restart of pipeline operations began at 5 p.m. on May 12, ending a six-day shutdown. On June 7, the Department of Justice announced that it had recovered 63.7 of the bitcoins from the ransom payment, a value of approximately $2.3 million.

JBS Meat Processing Company

On May 30, 2021, JBS S.A., a Brazil-based meat processing company which supplies approximately one-fifth of the global meat market, suffered a ransomware cyber attack. The attackers apparently used compromised system-access credentials to remotely disable JBS' IT networks and operations in the U.S., Canada, and Australia. All JBS-owned beef facilities in the U.S. were rendered temporarily inoperative because processing operations were not possible without normal access to IT and internet systems.

JBS paid the hackers an $11 million ransom in bitcoin. The FBI attributed the attack to REvil. Fortunately, JBS USA's ability to quickly resolve the issues resulting from the attack has been credited to effective cybersecurity protocols, redundant systems, and encrypted backup servers.

Kaseya LTD

On July 2, 2021, as many as 1,500 small to medium-sized companies around the world were affected by a supply chain ransomware attack centered on U.S. information technology firm Kaseya LTD. Kaseya provides IT management software solutions for both on-premises and cloud-based services to about 37,000 customers directly, and to over 800,000 more through managed service providers. Russian hacking group REvil claimed responsibility for exploiting vulnerabilities by injecting its ransomware into Kaseya's software. The distributed ransomware compromised Kaseya's customer operations, but Kaseya reported no evidence of compromise to its cloud-based services after quickly shutting down servers as a precaution.

Most Kaseya users affected were schools and small businesses such as dentists' or accountants' offices. For example, nearly 800 Swedish supermarkets and 11 New Zealand schools were closed for several days.

REvil demanded $70 million to restore all the affected data, but indicated willingness to temper their demands in private conversations. On July 21, 2021, Kaseya received a universal decryption key from a third party, and it was distributed to the impacted companies to restore operations. The company stated that no ransom was paid to obtain the key.

City of Oldsmar, Florida Water Plant

On February 5, 2021, the drinking water treatment facility for the City of Oldsmar, Florida was the target of a cyber attack. The municipally-owned facility provides water to businesses and 15,000 residents in Pinellas County, Florida. To obtain access to the SCADA system, unidentified cyber actors exploited cybersecurity weaknesses such as poor password security, an outdated operating system, and unprotected internet-based remote access software. This access enabled the cyber actors to increase the amount of caustic sodium hydroxide (lye), used in the water treatment process. Plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation. No customers or company personnel were harmed. Oldsmar's treatment process remained unaffected and continued to operate as normal, but the incident provided motivation nationwide for small water utilities to address the very basic protection weaknesses that were exploited.

Apache Log4j

On December 9, 2021, a vulnerability was found in one of Apache Software Foundation's publicly-released open-source codes. Log4j is a software library that records events and error messages as they occur when certain software is run. Log4j is essential to programmers for changing, debugging, or improving software performance and is integrated into countless applications. It is used by major cloud services such as Apple, Google, Microsoft, and Amazon, as well as platforms like Twitter. The Log4j vulnerability allowed ransomware attackers to take over any internet-connected service that uses specific versions of Log4j and execute malicious code to enter corporate networks around the world. In one confirmed compromise, attackers were able to gain access to a disaster recovery network and collect and extract sensitive data.

Organizations using Log4j may remain vulnerable to attacks for years. The Department of Homeland Security considers this an endemic ongoing vulnerability, and emphasized that all stakeholders must remain vigilant against the risks. Adequate protection necessarily includes identifying, mitigating, patching affected products using Log4j, informing end-users of products containing this vulnerability, and prioritizing software updates.

PIPEDREAM aka INCONTROLLER

Since being discovered in April 2022, cybersecurity experts continue to observe and track an OT-ICS malware known as PIPEDREAM. The discovery of PIPEDREAM is the first case of pre-emptive detection of a major attack targeting OT-ICS. No damage or interruption of operations was caused, but the discovery of this threat has prompted widespread response by potential targets. PIPEDREAM is a malware attack framework with primary focus on critical infrastructure equipment and related technologies in oil, gas, and electric power operations.

PIPEDREAM has been credited to a group named CHERNOVITE, which is believed to be a Russian state-sponsored threat actor.

According to CISA, advanced persistent threat actors have exhibited the capability to gain full system access to multiple ICS/SCADA devices. PIPEDREAM consists of cyber tools used by these actors for reconnaissance, manipulation, and disruption of ICS/SCADA devices, safety instrumented systems, programmable logic controllers, and computers that communicate with them. PIPEDREAM is difficult to detect and includes features such as the ability to spread from controller to controller.

Equipment found in liquefied natural gas and power generation industries have been the perceived focus of the detected attack, but it is possible that a wider set of targets could be subject to compromise. With full system access to ICS/SCADA devices, attackers could move laterally within the OT network to disrupt critical functions or devices.

Advanced persistent threat groups employing the PIPEDREAM malware appear to be learning from each other, and adopting tactics from previous attacks. Potential targets continue to proactively perform mitigation activities, such as monitoring their industrial environments for vulnerabilities, conducting active threat detection activities, reviewing cybersecurity advisories, and tracking recent intrusion tactics.

Saudi Aramco

In 2017, the Russian Central Scientific Research Institute of Chemistry and Mechanics deployed its TRITON OT-ICS malware against Saudi Aramco. Saudi Aramco, owned by the government of Saudi Arabia, is one of the largest oil companies in the world. Hackers used the software to manipulate ICS 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, but inadvertently triggered a shutdown of operations using an attack framework designed to interact with safety system controllers. These controller systems provide remote computerized process control for companies in the energy, manufacturing, and mining sectors.

Attackers gained remote access to at least one engineering workstation and deployed TRITON in an apparent attempt to reprogram or manipulate the safety instrumented system controllers. No damage was incurred and no ransom demands were made. The event was widely seen by all critical infrastructure sectors as a warning sign that the sophistication of OT-ICS cyber attacks is increasing.

Substation Attacks - Duke Energy Carolinas, LLC

On December 3, 2022, a coordinated physical security attack disabled two substations in Moore County, North Carolina. Rifle fire was used to damage critical substation components leaving about 45,000 customers without power. Service to all customers was restored within five days. The attack is being investigated by local, state, and federal law enforcement.

A similar attack on Pacific Gas & Electric's Metcalf transmission substation near San Jose, California was detailed in Commission staff's 2014 report. On April 16, 2013, 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.

2.6 Federal Initiatives and Cooperative Resources

2.6.1 Executive Orders

In recent years, a number of Presidential executive orders and other federal agency initiatives have been aimed at mitigation of cybersecurity risks. One key area of focus has been on prohibition of purchases or use of certain goods and services from foreign adversaries which pose a supply chain security risk. Another area of focus has encouraged development and use of SBOMs, an inventory of components and dependencies (e.g., open-source software and other third-party libraries) that allows end users to identify vulnerabilities, validate integration, and comply with regulatory requirements. DOE also launched a cybersecurity initiative to address ICS/OT network security through deployment of technologies providing threat visibility, detection, warnings, and response capabilities.

2.6.2 Infrastructure Investment and Jobs Act

On November 15, 2021, H.R. 3684 *Infrastructure Investment and Jobs Act* was signed into law. Selected provisions relating to the security and resiliency of the BES are displayed in **Exhibit 2.**

Infrastructure Investment and Jobs Act
Cybersecurity Summary
2021

Section	Description
Enhancing grid security through public-private partnerships	Requires the Secretary, in consultation with State regulatory authorities, industry, NERC, and other relevant federal agencies, to carry out a program to promote the physical and cybersecurity of electric utilities, with priority provided to utilities with fewer resources. Requires a report to Congress on improving distribution cybersecurity.
Energy Cyber Sense program	Establishes a voluntary Energy Cyber Sense Program to test the cybersecurity of products and technologies intended for use in the BES.
Incentives for advanced cybersecurity technology investment	Directs FERC to initiate rulemaking to develop incentives that would encourage investment in cybersecurity technology and participation in cybersecurity threat information sharing programs.
Rural/Municipal utility advanced cybersecurity grant and technological assistance program	Directs the Secretary of Energy to establish the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program to provide grants and technical assistance for utilities to detect, respond, and recover from cybersecurity threats. Authorizes $250M for FY22-26.
Enhanced grid security	Creates programs to develop advanced cybersecurity applications and technologies for the energy sector, enhance and test emergency response capabilities of DOE, and increase functional preservation of electric grid operations or natural gas and oil operations in the face of threats and hazards. Authorizes $250M over FY22-26 for the Energy Sector Cybersecurity R&D Program, $50M for FY22-26 for the Energy Sector Operational Support Cyber Resilience Program, and $50M for FY22-26 for Modeling and Assessing Energy Infrastructure Risk.
Cyber Response and Recovery Fund	Funds $20M per year for 5 years. The provisions allow the Secretary of Homeland Security to declare a Significant Incident following a breach of public and private networks. The fund allows CISA to provide direct support to public or private entities as they respond and recover from significant cyber attacks and breaches.

The State, Local, Tribal, and Territorial Grant Program (SLTT)	Provides a total of $1B allocated over 4 years ($200M FY22, $400M FY23, $300M FY24, $100M FY25). Funds are available until expended. This will establish a new grant program to provide Federal assistance to SLTT entities. The program will be administered by FEMA in consultation with CISA acting as the subject matter expert.
DHS Science and Technology Directorate for R&D.	Allocates $31.5M per year over 5 years. These funds will include support for specific areas of research related to risk assessments; cybersecurity vulnerability testing; and positioning, navigation, and timing capabilities.
CISA Sector Risk Management	Funds one-time investment of $35M in FY22 for CISA to establish a capability to oversee and execute cross-sector governance to support CISA's national cross-sector coordination role, established in FY21 NDAA.
Office of the National Cyber Director (NCD)	Allocates $21M in FY22 for a newly created office of the NCD, serving as a principal advisor to the President on cybersecurity policy, and cybersecurity engagement with industry and international stakeholders.

Exhibit 2 *Source: Senator Cantwell, Infrastructure Investment and Jobs Act Summary*

2.6.2 Cooperative Resources

Electric utilities maintain cybersecurity personnel who coordinate with national labs, government agencies, industry partners, vendors and law enforcement officials to best protect the U.S. electric power grid. The sharing and receiving of cybersecurity intelligence is augmented from the following key organizations:

- DOE's Cybersecurity Risk Information Sharing Program (CRISP) is a public-private data sharing and analysis platform managed by NERC's Electricity Information Sharing and Analysis Center (E-ISAC) to facilitate sharing of cybersecurity threat information among energy sector stakeholders. Through partnership and energy sector owners and operators, CRISP leverages advanced sensors and threat analysis techniques developed by DOE to better inform the energy sector of high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental U.S. electricity subsector customers.

  E-ISAC serves as the primary channel for gathering and analyzing security information from platforms such as CRISP. E-ISAC receives and coordinates incident reports and communicates mitigation strategies for energy sector stakeholders.

- The Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry. The ESCC directed the formation of the Cyber Mutual Assistance (CMA) Program. The Program is composed of electric and natural gas industry cyber experts, including municipalities and electric cooperatives, which can provide voluntary assistance to each other in advance, or in the event, of a cyber emergency that disrupts electric or natural gas services.

- Cybersecurity and Infrastructure Security Agency (CISA) provides alerts intended to provide timely information about current security issues, vulnerabilities, and exploits. In August 2021, CISA established the Joint Cyber Defense Collaborative (JCDC), a public-private partnership that proactively gathers, analyzes, and shares actionable cyber risk information to enhance cybersecurity planning, cyber defense, and response.

- The National Security Agency (NSA) is an intelligence agency within the Department of Defense responsible for gathering intelligence from electronic communications to protect national security systems from unauthorized access by internal and foreign adversaries.

- North American Transmission Forum (NATF) promotes safe and reliable electric transmission system operations through various programs. NATF collaboratively works with member utilities in areas such as improving cybersecurity practices and assisting with NERC reliability standards compliance. For example, guidelines were published to address the new NERC CIP-013 reliability standard regarding supply chain risk management.

- Electric Power Research Institute (EPRI) is a trade organization that conducts research, development, and demonstration projects focusing on electricity generation and delivery. EPRI's current cybersecurity research for power delivery and utilization includes artificial intelligence to automate threat management for integrated security operations centers, transmission and distribution and substation and control center security, OT threat management and security metrics, and DER management system security.

3.0 NERC Compliance Standards

3.1 NERC CIP Reliability Standards

From 2008 to date, FERC has approved 13 CIP reliability standards to protect critical components of the BES from cyber and physical security attacks. Each CIP standard is broken down into cyber and physical security protection requirements. The requirements specify required measures for identifying critical cyber assets, developing security management controls, training, facility security, and use of firewalls. Examples of cybersecurity measures to prevent cyber attacks include:

- Least-privilege, role-based access – allowing precisely the amount of network privilege that is necessary for a user to perform a job.
- Password management and multifactor authentication – set procedures for storing and managing passwords often requiring multiple authentication steps to gain network access.
- Configuration monitoring – automated means to search for and detect server and application configuration changes in network environment.
- Automated patch analyses – ongoing monitoring of completing needed software and operating system patches and addressing security vulnerabilities within a program or product.
- Logging and situational awareness – ongoing monitoring and maintaining a record of IT events to minimize operational disruption and downtime.

The format for each CIP reliability standard 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 3** provides a list of the 13 CIP reliability standards currently subject to NERC enforcement, the corresponding current version number approved by FERC, and the title and purpose of each CIP.

New and Revised NERC CIP Reliability Standards 2018-2022

The initial NERC reliability standards, CIP-002 through CIP-009, were approved by FERC and became effective in 2008. CIP-010 and CIP-011 were added and became effective in 2014, closely followed by CIP-014 in 2015. NERC CIP-013 became effective in 2020 requiring responsible entities to implement security controls for supply chain risk management. Specifically, CIP-013 requires these entities to have plans that identify and assess cybersecurity risks to the BES from vendor products or services. The plans must address cybersecurity protections such as software integrity and authenticity, vendor remote access, information system planning, and vendor risk management and procurement controls.

NERC Critical Infrastructure Protection Reliability Standards 2022			
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	8	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	7	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	6	Incident Reporting and Response Planning	Mitigate the risk to the reliable operation of the BES as the result of a cybersecurity 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	4	Configuration Change Management and Vulnerability Assessments	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-012	1	Communications between Control Centers	Protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
CIP-013	2	Supply Chain Risk Management	To mitigate cybersecurity risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.
CIP-014	3	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 3

Source: NERC CIP Reliability Standards

In 2020, FERC revised CIP-005 and CIP-010 to work in tandem with the new CIP-013 supply chain risk management requirements. CIP-005 now requires system owners and operators to log and monitor vendor remote access to ICS hardware, software, and other networking services associated with High and Medium Impact BES Cyber Systems.

CIP-010 now includes improved controls such as requiring system owners and operators to verify the identity of the software source and to confirm the integrity of all software and patches prior to installation. The 2020 revisions to these standards apply to critical cyber assets, defined as any programmable electronic devices and communication networks including hardware, software, and data. Examples of critical cyber assets 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.

In 2020, CIP-003 was revised to require security controls for transient electronic devices such as USB flash drives, laptop computers, and other portable devices used at Low Impact BES Cyber Systems.

In 2021, CIP-008 was expanded to require not only the reporting of actual compromises but also *attempts* to compromise an electronic security perimeter, physical security perimeter, an electronic access control or monitoring system for a High or Medium Impact BES Cyber System. As defined by NERC, a reportable cybersecurity incident is one that compromises, disrupts, or attempts to disrupt:

- Operation of a BES Cyber System
- Electronic Security Perimeter of a High or Medium Impact BES Cyber System
- Electronic Access Control or Monitoring System of a High or Medium Impact BES Cyber System

In 2022 CIP-012 became effective, imposing security requirements regarding communications between control centers. The NERC Supply Chain Standards, collectively CIP-005, CIP-010, and CIP-013, were revised to include electronic access control and monitoring systems, and physical access control systems.

3.2 Emergency Operations Standards

Section 215 of the Federal Power Act required NERC to develop mandatory emergency operations standards that are subject to FERC review. Emergency Operations (EOP) reliability standards address preparation for emergencies, necessary actions during emergencies, and system restoration and reporting following disturbances.

- EOP-004-4 (Event Reporting) requires reporting of physical security events including loss of control center capabilities, transmission loss, and generation loss).

- EOP-005-3 (System Restoration from Blackstart Resources) requires plans, facilities, and personnel are prepared to enable system restoration from blackstart resources.

- EOP-006-3 (System Restoration Coordination) requires plans are established and personnel are prepared to enable effective coordination of the system restoration process.

- EOP-008-2 (Loss of Control Center Functionality) requires operating plan, backup control center designation, and backup functionality including capability for monitoring, control, logging, and alarming.

- EOP-010-1 (Geomagnetic Disturbance Operations) requires Geomagnetic Disturbance (GMD) operating plans, processes, and procedures.

- EOP-011-1 (Emergency Operations) requires plans to mitigate operating emergencies within a reliability coordinated area.

3.3 Transmission System Planning Standards

NERC's Transmission System Planning Standards (TPL) require transmission systems to be planned and designed to meet specified criteria. The TPL 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.

In 2016, FERC approved reliability standard TPL-007 to establish requirements for transmission system planned performance during GMD events. An electromagnetic event can result from a naturally occurring, large-scale GMD caused by severe solar weather, or from human-made sources such as the detonation of a nuclear device at high altitude that can impact the electric power grid. A 2020 revision of TPL-007 requires owners and operators of the BES to conduct and develop corrective action plans for vulnerabilities identified through GMD assessments.

4.0 Florida Power & Light Company

Florida Power and Light Company (FPL or the company), a subsidiary of NEE operates approximately 32,000 megawatts of generating capacity. The company provides electric service to 5.8 million customers, representing more than half of Florida's homes and businesses. FPL's bulk transmission system, including both overhead and underground lines, is comprised of 9,174 circuit miles of transmission lines. The integration of its generation, transmission, and distribution systems is achieved through 832 substations in Florida.

4.1 Cybersecurity Management Oversight

4.1.1 Integration of Gulf Power Company

Prior to acquiring Gulf Power Company from its parent, Southern Company, NEE engaged multiple third-party evaluations of Gulf Power's cybersecurity systems. Upon acquisition in 2019, NEE, FPL, and Gulf Power Company began assessing Gulf Power's cybersecurity system controls to plan the full operational transition. The Gulf Power substation landscape included 39 transmission substations and 97 distribution substations.

The integration of Gulf Power/Southern Company Systems focused on the following key areas:

- Assessing transmission infrastructure
- Evaluating computer systems for monitoring and control of Gulf Power
- Modifying substation and smart grid communication
- Testing operational integration
- Modifying independent regulatory certifications, NERC/FERC entity certification
- Transitioning Gulf Power to FRCC Reliability Coordinator footprint

FPL collaborated with the Gulf Power/Southern Company IT team to extract substation components from Gulf Power/Southern Company's asset management program. The extraction included asset attributes, such as substation name, physical location of the asset within the substations, manufacturers, model numbers, etc. The extracted data was transferred to the FPL asset management database.

The distribution control center operations for Gulf Power's former service territory, now known as FPL's Northwest Region, continued to operate out of Pensacola but transitioned to use FPL's Emergency Management and Distribution Management systems in July 2020. The transmission system control center integration cutover was accomplished in July 2022.

Similarly, Southern Company and Gulf Power physical security protections were evaluated and migrated to the NEE Enterprise Physical Security environment. Following assessment and modifications, the physical security protections were adopted under the Enterprise Physical Security Program.

4.1.2 Cybersecurity and Physical Security Leadership

NEE's and FPL's Cybersecurity organization is headed by the Senior Director of IT Security. The position's responsibilities include incident detection and defense, identity and access management, cybersecurity assurance, governance, risk management, and NERC CIP standards compliance. Overall adherence to the CIP standards falls under the authority of the CIP Senior Manager, who also is the Executive Vice President of FPL Power Delivery.

The Corporate Security organization is headed by the Senior Director, Security Aviation. The position's responsibilities include directing corporate-wide physical security policies and programs (excluding nuclear), and investigating malicious acts taken against the company. The Senior Director leads a team of security personnel, maintaining close relationships with law enforcement, and federal, state, and local regulatory agencies.

NEE and FPL operate dedicated 24x7 cyber and physical security operations centers. The Advanced Cyber Defense Center monitors and protects against cyber threats. The Security Operations Center team is responsible for physical security across the company. These teams reside in separate business units, using a common security architecture interconnecting both through real-time intelligence sharing, threat identification, and incident response.

4.1.3 Policies and Procedures

The cybersecurity protection program at FPL leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the NERC CIP standards to manage cyber and physical security risks. The following core strategies are the foundation of the NIST framework:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to information technology assets
- **Protect** – Implement safeguards that protect information technology assets
- **Detect** – Deploy solutions to identify occurrences of a potential cybersecurity event
- **Respond** – Take appropriate action regarding detection of a potential cybersecurity event
- **Recover** – Execute and test plans to restore all capabilities impaired by a potential cybersecurity event

The objective of the NIST framework and core strategies is to evaluate the maturity of the company's cybersecurity program and develop policies and procedures to coordinate and mitigate cybersecurity risks.

To provide a structure for enforcing compliance with the NERC CIP reliability standards, FPL adopted a pyramid model or "Policy Stack" approach used in the development of policies and procedures. As shown in **Exhibit 4**, the Policy Stack consists of five levels, with the highest level being the overarching policy or mission statement. The policy statement and goals guide

operations in performing tasks required by NERC CIP requirements. The statement applies to all employee and contractor personnel who have access to, or are responsible for the operation, protection and maintenance of applicable BES cyber assets.

The next level is comprised of the multiple NERC CIP standards (CIP-002 through CIP-014) that establish compliance requirements. The "Procedures" level identifies the managerial, administrative, technical controls, and processes supporting the NERC CIP standards. The remaining levels are the Work Instructions, and Supporting Documents and Systems that include the detailed activities, process flows, and evidence that cybersecurity controls are implemented.

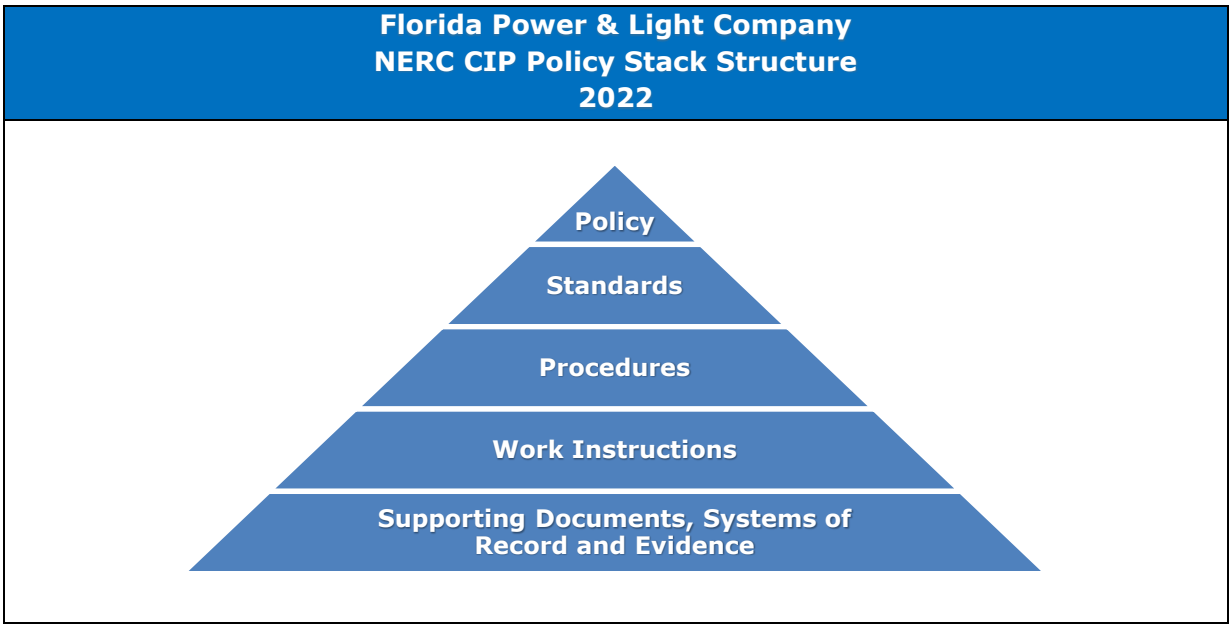

Exhibit 4 *Source: Document Request 1.3*

4.2 Cybersecurity Costs

The evolution of new and more sophisticated attack vectors has resulted in increased cyber-protection expenditures for all electric utilities with extensive BES connectivity. While no cyber attacks on the U.S. bulk grid have caused significant power outages, the ever-changing threat environment forces utilities to continually reassess protections and resource allocations.

FPL's cybersecurity-related expenditures have trended upward at a steady pace over the last several years. Cyber-protection investment and expenditures are also driven in part by regulatory requirements from agencies such as FERC, NERC, DOE, and DHS. Personnel costs make up a large share of FPL's cybersecurity expenses and world-wide demand for uniquely-skilled professionals is extremely high.

4.3 NERC CIP Compliance

4.3.1 SERC Audits

On behalf of NERC, SERC performs CIP compliance audits over a three-year period, providing a rigorous, systematic, and objective examination of FPL's CIP compliance-related records and activities. SERC CIP audits consist of site assessments, review of programmatic documentation and evidence, and on-site interviews of subject matter experts. Upon completion, the utility responds to any deficiencies identified by SERC, and corrective actions proposed are approved and documented to ensure compliance. Three audits of FPL's compliance with selected CIP reliability standard requirements were performed in 2018, 2019 and 2022. Resolution of all findings and approved remedial actions is complete or nearing completion for these audits.

4.3.2 Self-Reporting

As part of the NERC Compliance Monitoring and Enforcement process, NERC relies on FPL to self-report potential non-compliance issues through its structured review process. While the process is voluntary, the practice is viewed favorably by the regulator and demonstrates a strong company culture of compliance. FPL follows an enterprise-wide procedure ensuring a standardized process is used for tracking and filing a self-report. FPL identifies and self-reports potential compliance deficiencies to SERC as they are discovered. SERC reviews and takes into consideration the self-reported non-compliance issues in developing findings, approving corrective actions, and some instances imposing penalties. FPL develops and follows a mitigation plan to re-establish compliance and prevent recurrence.

4.3.3 CIP Center of Excellence Program

In 2020, FPL performed a comprehensive analysis of its approach to CIP compliance. The analysis recommended development of a centralized CIP program to drive efficiencies with focus on assuring compliance activities are successfully executed across all business units. This program would work to eliminate silos between business units, improving information exchange to optimize compliance performance.

In response to the analysis, FPL launched its NERC CIP Center of Excellence Program in 2021. The program is based on three focus points for compliance: Risk Management, Information Management, and Program Management. FPL uses automated tools and a score-carding process to track compliance with each CIP reliability standard requirement. The goal of the program is to reduce non-compliance risks, improve information quality, and strengthen the company's SERC audit readiness.

4.4 Self-Assessment Tools

To protect against cybersecurity threats, FPL conducts various self-assessments of its posture.

4.4.1 Cybersecurity Capability Maturity Model

FPL uses DOE's C2M2 voluntary self-assessment model to monitor cybersecurity program growth and development. The model allows the company to assess and plan overall program

maturity level. The evaluation can help participants identify and prioritize gaps in security capability and develop solutions.

FPL conducts a C2M2 assessment biennially with the support and oversight of a third-party assessment consultant. Findings and remediation plans are input to the company's risk register and are tracked through the risk management process.

In April 2021, the DOE updated the C2M2 to address new technologies such as cloud computing, mobile, artificial intelligence, and evolving threats such as ransomware and supply chain risks. FPL's most recent C2M2 evaluation, completed in 2022, included a first-time assessment of the IT processes in FPL's Northwest Region (Gulf Power). It also included a secondary assessment to gauge a baseline maturity indicator level measurement for the OT environment.

4.4.2 EEI Culture of Security Tool

As cybersecurity threats continue to persist and grow, utilities must maintain and continuously adapt a security-centered corporate culture. EEI provides a "Culture of Security" self-assessment tool for utilities. In recent years, FPL has performed multiple EEI Culture of Security assessments for its own self-evaluation.

This activity enables FPL to examine the maturity level of the present security culture. The assessment allows utilities to better understand security as a fundamental component of corporate culture and drives continuous improvements and innovative approaches.

The assessment is divided into five operational areas:

- Security Governance, Risk, and Workforce Management
- Cybersecurity Protections
- Physical Security Protections
- Response, Recovery, and Exercises
- External Partnerships and Information Sharing

These are scored against four performance maturity levels ranging from "initiated" to "optimized." The outcome of Culture of Security assessments directly influences future projects and budgeting to further develop FPL's overall cybersecurity program.

Most recently, the 2022 assessment indicated continued improvement towards implementation of the EEI suggested standards.

4.4.3 Internal Audits and Consultants

FPL performs internal audits and assessments to determine the adequacy of cyber and physical security internal controls. These address specific security-related issues such as patch management, insider risk management, network monitoring, and threat hunting.

The company also frequently engages external consultants to provide targeted cybersecurity protection services and vulnerability assessments. These engagements have assessed cloud

security, environment protection, compromise detection, management vulnerability, OT threat detection, external penetration, and NERC CIP readiness.

4.4.4 Metrics

FPL cybersecurity risks are monitored through tailored performance indicators that provide quantitative assessment and measurement. Metric results are provided to multiple levels of management for awareness and monitoring. Metric performance trends are examined to identify off-target results and trigger investigation and corrective action. The company presently reports and assesses the following cyber and physical security indicators:

- Phishing/reporting click rate
- OS version life cycle compliance
- Patching compliance
- Policy exceptions
- Progress on remediation plans for findings tracked in risk registers
- Vulnerability remediation
- Effectiveness of Cybersecurity Technology in blocking/protecting corporate assets/users
- Alert/incident volume monitored by the 24x7 Advanced Cyber Defense Center

4.5 Risk Management

4.5.1 Cybersecurity Maturity Model Certification

To assess its cybersecurity readiness, FPL has incorporated the Department of Defense Cybersecurity Maturity Model Certification (CMMC) program as a foundational component of its Cybersecurity Risk Management program. The CMMC program is derived from multiple cybersecurity standards and frameworks, including NIST, and was originally created to protect the Department of Defense from intellectual property breaches that could weaken its operations.

FPL uses its Cybersecurity Risk Management program to assess the maturity level of its cybersecurity processes and practices. Each maturity rating level indicates a higher degree of protection capability. The Cybersecurity Risk Management program further involves assessing all vendors, subcontractors, and service providers, including compliance with applicable NERC CIP reliability standards and industry best practices. FPL senior managers (CIO, CISO, CFO, and CEO) receive periodic reports to ensure compliance with regulatory requirements.

4.5.2 Risk Registers

The NIST Cybersecurity Framework assists utilities to develop and use risk registers. Risk registers track and communicate risk information, including description of each risk, impact, probability of occurrence, potential damage, mitigation strategy, risk prioritization, and the responsible business unit owner.

FPL maintains and manages the cyber and physical security risk registers described below. Status reports are included in an overall NEE corporate risk register and reviewed quarterly by NEE's Corporate Risk Committee for security protection awareness.

IT Risk Register

The Cybersecurity Risk Management team maintains a risk register to track all identified IT risks, findings, and mitigation plans to completion. The issues and findings input to the risk register are the findings and results of internal and external reviews, such as C2M2 and industry/consultant assessments. These findings are documented and tracked through the Governance Risk and Compliance platform, a software application that aligns IT with business unit goals while managing risks and complying with NERC CIP reliability standards and other industry and government regulations.

OT/ICS Risk Register

FPL's OT/ICS risks are maintained and managed by a third-party consultant. The scope of OT/ICS monitoring includes all business units. The consultant maintains a built-in OT/ICS risk register layered with the IT environment. The register captures and mitigates potential threats that may pivot to the OT/ICS environment and promotes effective communication between IT and OT personnel and devices to mitigate OT security risks.

Corporate Security Physical Risk Register

FPL's Corporate Security and Power Delivery teams maintain and manage a risk register for physical security to track identified physical security risks and mitigation plans. As required by CIP-002, FPL employs a risk-based methodology to identify transmission facilities critical to the reliability of the grid. Criticality is based on potential impact the loss of a facility may have to the reliability of the FPL transmission system. Based on the determined criticality, the company employs physical security protections pursuant to CIP-006 and CIP-014.

FPL also manages physical security risk through facility security reviews, vulnerability assessments, and inputs to the Corporate Security Risk Register. A final report is shared with the local business unit team leader for follow-up action if necessary.

4.6 Cybersecurity Protection Trends and Issues

4.6.1 Convergence of IT and OT

FPL currently manages the cybersecurity risks involved in the convergence of its IT/OT networks through multiple layers of security to ensure system reliability and resiliency. Converged assets are tracked by a monitoring software that logs information and part numbers to facilitate sourcing currently held hardware and software IDs. Both physical and electronic security devices are used within the converged IT/OT network which are monitored by security operations analysts.

The company also employs firewalls, intrusion detection devices, and built-in redundancies and network segmentation to block and isolate unwanted traffic to protect against internal and external security threats.

4.6.2 Supply Chain Protections

To protect against supply chain compromise, FPL has updated supply chain standards to reflect current requirements, added protections into its contracts with third-party vendors, and continue

to work with industry partners to execute upgrades and countermeasures as they become available.

Since the public announcement of the SolarWinds attack, utilities using SolarWinds software were prompted to search systems for evidence of malware intrusion. FPL initiated an investigation and determined that operations were not impacted. Although the SolarWinds compromised versions were not in use, the company followed the guidance included in directives and advisories from entities such as CISA, FireEye, Microsoft, and NSA to mitigate any possible impact to corporate technology, OT environments, or through compromised suppliers.

FPL collects and reviews documentation on potential new vendors' security controls to proceed with a risk assessment. After approval from the company's Cybersecurity and Technology Risk team, the purchasing process continues. Approved vendors are subject to reassessments whenever the company renews services, licenses, or modifies the contractual terms and conditions with the vendor.

Upon completion of the vendor approval process, FPL routinely scans the company's assets and tracks vulnerabilities and remediation times. FPL monitors vendor connections via firewalls and intrusion protection systems, and uses tools capable of inspecting data packets that are incoming and outgoing. A third-party program assesses and categorizes vendors using risk-based priority ratings.

Software and Hardware Bill of Materials

Although not explicitly mandated in the NERC CIP supply chain standards, FPL requests software and hardware vendors to provide an SBOM/HBOM. The company's contract language also requires all vendors to apply industry best practice updates to antivirus and patching technology to manage the integrity of purchases to minimize security risk.

FPL uses a third-party Cybersecurity Risk Program to perform SBOM/HBOM third-party vendor risk assessments to enhance supply chain software and hardware security protections. The assessments include review of incoming software and hardware purchases and verification that vendors and suppliers do not purchase from companies on the U.S. Entity List.[8] Furthermore, FPL participates in the government's SBOM/HBOM initiatives run by Idaho National Labs.

Cloud Services Protections

Cloud-based services provide FPL with a shared pool of computing resources through service level agreements with third-party service providers to increase operational efficiencies and reduce costs. The use of cloud services, however, introduces a degree of cybersecurity risk.

To protect against these risks from external-facing cloud services, FPL requires multifactor authentication for users, monitors business-to-business connections via intrusion protection system software (e.g., firewalls), and uses asset management tools to scan and track vulnerabilities and remediation times. Detection capabilities are also supported by a third-party cloud security platform that breaks down the vendors into a risk-based priority. The company's

[8] The U.S. Entity List is a trade restriction list published by the United States Department of Commerce's Bureau of Industry and Security, consisting of certain foreign persons, entities, or governments.

24x7 Advanced Cyber Defense Center team monitors logs and alerts from its cloud platforms and engages any business partner if a suspected incident occurs.

4.7 Threat Detection Activities

The 24x7 Advanced Cyber Defense Center team is charged with the discovery and identification of anomalous cybersecurity activity. FPL's Insider Risk team is responsible for monitoring, detecting, and investigating suspicious activity by users who have authorized access to the company's information and assets. These teams employ multiple layers of monitoring of the network and review rules and signature-based alerts to identify potential threats.

FPL uses an automated IT threat detection tool to detect, triage, and respond to potential phishing attacks. A third-party consultant is employed to perform OT monitoring that provides threat detection and mitigation.

FPL's Cyber Assurance team conducts penetration tests to identify weaknesses or vulnerabilities in systems, networks, human resources, or physical assets. The team executes threat emulation, advanced engagements, controls testing, and vulnerability validation. Findings and recommendations are provided to owners and stakeholders upon completion and tracked in a centralized platform to ensure remediation accountability.

In addition, Corporate Security performs periodic physical security assessments of selected facilities or locations.

4.8 Incident Reporting and Response

FPL's Cybersecurity Incident Response Procedure documents the process for responding to cybersecurity incidents which includes instructions for required reporting. Pursuant to NERC CIP-008, the plan is used whenever a potential incident occurs and is tested at least once every 15 months.

FPL's CISRP guides compliance with the incident reporting and response requirements of NERC CIP-003 and CIP-008. An incident is reportable to DOE, E-ISAC, and DHS if it has compromised or disrupted, has the potential to compromise, or is an attempt to compromise a high or medium impact BES cyber system.[9] The minimum data that must be reported is the functional impact, the attack vector used, and the level of intrusion that was achieved or attempted. NERC CIP reporting must be completed within the following timeframes:

- One hour for a reportable cybersecurity incident
- End of next calendar day for an attempt to compromise an applicable system
- Within seven calendar days for any updates (if necessary) to the initial notification

[9]A single completed Form DOE-417 may be electronically submitted to the agencies to satisfy the incident reporting requirement.

The CSIRP also assists in the reporting required in NERC EOP-004. The filing of Form DOE-417 is required to report any incidents and disturbances that might be triggered by a cyber and/or physical security attack. FPL must submit a completed form within the following timeframes:

- One hour if the incident causes electrical system operation interruption
- Six hours if the incident could have impacted electric power system reliability
- 24 hours of determination of an attempted compromise

Should FPL determine that an incident is cybersecurity related, the incident will be categorized and tracked as high, medium or low based on actual or potential impact. The categorization considers the impact to business operations and the confidentiality, integrity, and availability of information.

In case of a cyber or physical security incident that causes a significant outage, FPL will notify the Florida Department of Law Enforcement Fusion Center, Florida Division of Emergency Management, and the Commission (pursuant to Rule 25-6.018 F.A.C.)

On March 15, 2022 the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law. The new rule will require entities involved in critical infrastructure to report cyber incidents to CISA within 72 hours and any paid ransom demands within 24 hours. Although the new reporting requirements will not become effective until CISA's rulemaking process is completed, FPL voluntarily reports cyber incidents using CISA's web-enabled incident reporting system.

FPL follows NEE's Corporate Emergency Management Plan (CEMP) which specifies procedures for responding to threats and hazards. In the case of a major cyber or physical attack, the CSIRP turns over incident command to CEMP. The company has defined roles and responsibilities for key positions involved in Emergency Preparedness Plans. Its Emergency Response Organization, FPL leverages DHS National Incident Management System and Incident Command System as the standardized organizational structure for management of all incidents.

4.9 Incident Recovery

FPL's CSIRP guides compliance with the incident recovery requirements of NERC CIP-009 and EOP-005, EOP-006, EOP-008, EOP-010, and EOP-011 reliability standards. The company states that it adheres to all of the incident recovery requirements in the NERC reliability standards.

The IT business unit maintains FPL's Disaster Recovery Program. Application recovery plans are created and stored in a designated disaster recovery location. A central disaster recovery coordinator and team are responsible for reviewing and updating the restoration plan, identifying the support personnel required, and prioritizing the execution of the plan.

FPL uses automated tools and processes for backup and storage of information required to recover BES cyber system functionality. The company's recovery procedures for BES cyber systems contains the condition for activating recovery of BES cyber assets. The

following events and conditions would result in the use of the recovery procedure and/or work instructions:

- Any applicable identified BES cyber system becomes unavailable, cannot perform its function, and cannot be repaired.
- Unauthorized access of any applicable BES cyber system that affects the confidentiality, integrity or availability of those systems.
- Physical destruction or impairment of any applicable BES cyber system.
- Natural disaster that affects the High and Medium Impact BES cyber systems.

Corporate Security consolidates physical security recovery activities in its annual Business Continuity Plan. The plan provides detailed information on the activation and continuation of critical functions and processes for applicable business units. It includes a description of key strategies, contacts, and vital records to be used during an emergency allowing Corporate Security to maintain and sustain safe business operations.

The Disaster Recovery Program and the Business Continuity Plan ensure readiness of secondary locations available to take over the operation of critical functions from the primary location of the application or system. These secondary locations are tested annually. In the event of communication technology failure, the Disaster Recovery Program and Business Continuity Plan provide designated alternative forms of communication and facilities to report to for more information. To date, no activation of any recovery plans in response to a cyber or physical security incident has been required.

FPL is an active participant in EEI's Cybersecurity Mutual Assistance (CMA) Program. Although the company has not asked for assistance from the program, FPL continues to partner with other organizations to prepare for collaborative recovery efforts and information sharing.

5.0 Participation in Drills and Exercises

FPL performs response drills and exercises across business units and participates in voluntary programs in coordination with federal, state, and local regulatory agencies and emergency authorities.

FPL established a formal assessment program based on an annual cyber drill. In a mock cyber-attack scenario, cybersecurity analysts are subjected to quarterly technical assessments which challenge and measure technical aptitude and incident response capability.

FPL participates in NERC's GridEx, the biennial North American grid security exercise sponsored by NERC. GridEx tests industry-wide emergency response and recovery plans through simulated cyber and physical security attacks. FPL participated in GridEx VI in November 2021 with objectives to activate incident management response plans, enhance

coordination with government to facilitate restoration, identify interdependence concerns with natural gas and telecommunications sectors, and exercise response to a supply chain-based compromise to critical components.

The company collaborates with multiple government partners, vendors, industry groups, and regulatory entities to promote information and intelligence sharing and threat detection capabilities. Since 2018, FPL has conducted 10 physical security tabletop exercises in Florida with federal (FBI/DHS), state (FDLE/Fusion Centers), and local law enforcement/emergency personnel at substations pursuant to the NERC CIP-014 reliability standard. Activities have included an operational, safety, and security review of each location, and exercises of physical security threat scenarios.