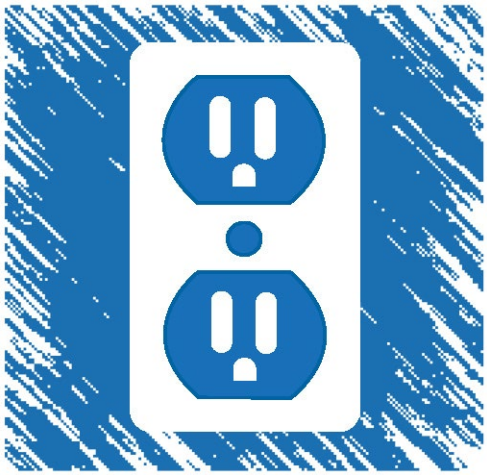

Review of

Cybersecurity Protections

Duke Energy Florida, LLC

Tampa Electric Company

February 2022

BY AUTHORITY OF

The Florida Public Service Commission
Office of Auditing and Performance Analysis

Review of

Cybersecurity Protections

Duke Energy Florida, LLC

Tampa Electric Company

Carl Vinson
Public Utilities Supervisor
Project Manager

Jerry Hallenstein
Senior Analyst

Vic Cordiano
Engineering Specialist II

February 2022

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

PA-20-01-001

TABLE OF CONTENTS

TABLE OF EXHIBITS

1.0 Executive Summary

This audit report addresses cybersecurity protections employed by Duke Energy FL, LLC (DEF) and Tampa Electric Company (TEC), over the period 2019-2021. In 2014 and 2018, the Florida Public Service Commission's (FPSC or Commission) Office of Auditing and Performance Analysis performed reviews of the cybersecurity and physical security protection measures used by the four largest investor-owned electric utilities (IOUs) in Florida.

Future audits will continue to periodically assess protections for other Commission-regulated IOUs.

1.1 Scope and Objectives

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

- Results of recent NERC audits, company internal audits, and external reviews assessing compliance with NERC Critical Infrastructure Protection (CIP) reliability standards
- Approach to risk management through compliance monitoring and internal control activities
- Implementation of new internal controls and compliance practices for new NERC CIP reliability standards
- Self-evaluation efforts and activities to enhance cyber and physical security protections and planning
- Cyber and physical security incident reporting internal controls as required by the North American Electric Reliability Corporation (NERC), Department of Energy (DOE), and FPSC
- 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 exploiting either supply chain 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 protection

- 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
- Separate tracking and identification of 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, Department of Energy, and other agencies have laid a solid foundation for protecting the most critical Bulk Electric System (BES) cyber assets operated by DEF and TEC.
- All assets of DEF and TEC within the Florida Public Service Commission's jurisdiction (i.e., below 100kV) 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 an effective, rigorous, and valuable enforcement tool.
- Though cyber attacks such as SolarWinds, Colonial Pipeline, and Kaseya have impacted industry operations, no cyber attack on any U.S. electric utility's systems has resulted in customer outages.
- DEF and TEC have assessed the impacts of recent attacks against utilities and are addressing their need for process and control improvements such as additional screening of third-party vendors and products.
- 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.
- Revisions to NERC CIPs increasingly require that selected protections previously mandated for only High Impact and Medium Impact BES cyber assets must also be provided for Low Impact BES cyber assets.
- Continuing efforts and costs lie ahead for DEF and TEC to comply with new and revised NERC reliability standards.

- Recent rate cases and resulting settlements with both DEF (FPSC Docket No. 20210016-EI) and TEC (FPSC Docket No. 20210034-EI) did not specifically address recovery of cybersecurity and physical expenses and investment.

- 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.

2.0 Background and Perspective

2.1 Limited FPSC Cybersecurity Protection Jurisdiction

The Florida Public Service Commission has limited jurisdiction over cybersecurity protection for the U.S. Bulk Electric System (BES). In fact, the FPSC's jurisdiction simply includes local distribution and smaller transmission facilities (those below 100 kV rating.) The Federal Energy Regulatory Commission (FERC) sets rules and standards for protecting the interstate transmission grid, which presents a higher-value target for attacks and disruptions. 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 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 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 2021	
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 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 attacks. Reports issued in 2014 and 2018 addressed protections of physical and cyber assets for Gulf Power Company, Florida Power & Light Company, Duke Energy-Florida, and Tampa Electric Company.

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 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.
- All assets of Florida IOUs within the Florida Public Service Commission's jurisdiction (i.e., below 100kV) fall outside of existing NERC CIP reliability standards.
- Selecting and implementing prudent, proportionate preparations against physical attack necessarily entails value judgments. Continuous vigilance and frequent reassessment of risk analysis and threat analysis should be employed by Florida IOUs.
- 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.

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

- To date, no successful efforts to disrupt[3] 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.

2.2 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 Industrial Controls Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) that monitors and controls plant equipment and power generation, and the Outage Management System (OMS) that provides real-time insight regarding customer outages and repair status.

With the advancement of new technologies, electric utilities such as DEF and TEC are moving forward with converging IT and OT. By doing so, processes are streamlined allowing for greater efficiencies such as improved data collection for operational decision making and real-time system degradation warnings to reduce repair time. However, the convergence of IT with OT opens the door for the OT network to become more vulnerable to cybersecurity threats and attacks. A successful attack on a utility's OT network has substantial potential to bring down the power grid for it and other utilities in the state.

Effective communication between IT and OT personnel and devices can mitigate the increased risk of OT compromise. DEF and TEC continue to implement cybersecurity OT protections to manage and monitor system access, track OT assets, detect malicious activity, and implement network segmentation.

[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.

2.3 Supply Chain and Cloud Services Threats

Cybersecurity threats facing electric utilities include the typical threats that plague other industries: malware, e.g., viruses, worms, trojans, spyware, and ransomware. Today, cybercriminals including nation-state actors, increasingly target large firms for ransomware payoffs and/or to cause infrastructure damage and shutting down operations.

Cybercriminals increasingly target supply chain vulnerabilities to launch ransomware attacks. Of necessity, utilities' heavy reliance on numerous vendors for system software and hardware opens the door for the introduction of malware into either IT or OT systems. 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. As IT and OT converge, 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. It also revised CIP-005 and CIP-010. These standards became effective on October 1, 2020, and require owners and operators of the BES to develop and implement supply chain management security controls protecting ICS hardware, software, and computing and networking services. These standards cover the following key security objectives:

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

One risk mitigation measure is to request that the vendor provide a Software Bill of Materials (SBOM) for all components of the software and/or firmware that were developed by third parties whether purchased or open source. A SBOM allows the entity to identify components known to present risks and hold the vendor accountable for providing patches for those components, when available and applicable.

Increased interest in SBOMs being provided by vendors may provide increased 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 being sold. Like nutritional information required in food product labelling, SBOMs will give purchasers greater insight into the contents of products being consumed so that associated risks can be considered. In the future, CIP-013 or other regulatory measures may be revised to require SBOMs or equivalent product information.

Another growing risk in the electric utility industry is the increasing use of cloud computing services. To streamline solutions and avoid the large expense of operating their own data centers, utilities are turning to third-party cloud service providers. Cloud computing provides entities with additional computer system resources such storage space, network bandwidth, and applications. However, by migrating to the cloud, utilities necessarily relinquish some cybersecurity responsibilities to a third party.

2.4 Distributed Energy Resource Deployment Threats

Increasing deployment of Distributed Energy Resources (DERs) introduces potential challenges for electric utilities. DERs are small, modular, energy generation and storage technologies, such as wind, rooftop solar, electric vehicles, and battery storage that provide electric capacity or energy where you need it. Typically, DERs produce less than 10 megawatts of power. Developing a risk management plan for DER-related risks is becoming necessary as DER use grows.

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

Increasing DER deployment as systems become more aggregated provides a target of opportunity for cyber attack aimed at system disruption. Some estimates forecast that the cumulative DER capacity in the U.S. could reach 387 gigawatts by 2025.

2.5 Notable Recent Cybersecurity Attacks

Recent notable IT/OT incidents are discussed in detail below. Each of these incidents holds implications for Florida IOUs and provides lessons learned to be considered.

SolarWinds (IT Compromise)

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 software developer SolarWinds, inserting malware into an update being developed for distribution to customers using SolarWinds' Orion business software. The supply chain attack allowed the 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.

Affected organizations worldwide included NATO, the U.K. and U.S. governments, the European Parliament, Microsoft, and others. SolarWinds stated that its customers included 425 of the U.S. Fortune 500, 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, as well as hundreds of universities and colleges worldwide.

Colonial Pipeline (IT Compromise)

On May 7, 2021, Colonial Pipeline, a pipeline system that carries gasoline and jet fuel mainly to the southeastern United States, suffered a ransomware cyber attack by Russian-based hacking organization REvil and a closely-associated ransomware group called DarkSide. To contain the attack, Colonial shut down its pipeline on the same day as a precaution due to a concern that the hackers might have obtained information allowing them to carry out further attacks on vulnerable parts of the pipeline. While the OT systems were not affected, the company's IT billing system was compromised. It 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 then sent Colonial Pipeline a software application to restore its network, which 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 (IT Compromise)

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 credentials to remotely access and 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, a sophisticated Russian ransomware organization. Fortunately, JBS USA's ability to quickly resolve the issues resulting from the attack has been credited to its cybersecurity protocols, redundant systems, and encrypted backup servers.

Kaseya LTD (IT Compromise)

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 businesses 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. Although Kaseya reported no evidence of compromise to its cloud-based servers, the company did shut down the servers as a precautionary measure.

Within an hour of discovering the attack, Kaseya shut down access to the potentially-compromised software. Most of those affected were schools and small businesses such as dentists' or accountants' offices. For example, in Sweden and New Zealand, nearly 800 supermarkets and 11 schools were closed for several days, respectively.

REvil demanded $70 million to restore all the affected businesses' data, although they indicated a 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 a ransom was not paid to obtain the key.

Saudi Aramco (OT Compromise)

In 2017, a malicious software known as "Triton" was deployed at Saudi Aramco, owned by the government of Saudi Arabia and 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 and inadvertently shut down operations using an attack framework designed to interact with Triconex Safety Instrumented 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 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 and no ransom demands were made. However, the event was widely seen by all critical infrastructure sectors as a warning sign that the sophistication of attacks aimed at OT systems was rapidly increasing.

City of Oldsmar, Florida Water Plant (OT Compromise)

On February 5, 2021, the drinking water treatment facility in 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. Unidentified cyber actor(s) exploited cybersecurity weaknesses such as poor password security, an outdated operating system, and/or unprotected internet-based remote access software to obtain access to the SCADA system. This access enabled the cyber actor(s) 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. As a result, the water treatment process remained unaffected and continued to operate as normal.

2.6 Federal Government Cybersecurity Initiatives

2.6.1 Presidential Executive Orders and Memorandum

In recent years Presidential Executive Orders regarding cybersecurity and critical infrastructure have been used by Presidents Trump and Biden to initiate policy initiatives and action by federal agencies playing key roles in cybersecurity protection. Recent executive orders impacting Florida's electric investor-owned utilities and their cybersecurity protections are summarized below.

Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain

Order 13873, issued May 15, 2019, addresses cyber-enabled malicious actions of foreign adversaries via economic and industrial espionage to exploit vulnerabilities in supply chains and information technologies. The Order declared these threats a national emergency and instituted prohibition of purchases of certain goods and services posing an undue risk of catastrophic effects on the security or resilience of U.S. critical infrastructure or the nation's economy.

The order addresses transactions involving information and communications technology or services either designed, developed, manufactured, or supplied by a foreign adversary, or that were subject to the jurisdiction or direction of a foreign adversary.

Executive Order 13920: Securing the United States Bulk-Power System

This order, issued May 1, 2020, addresses the problem of foreign adversaries creating and exploiting vulnerabilities of the bulk power system (BPS). To address this threat, the order takes steps to protect the security, integrity, and reliability of BPS equipment used and supplied to the U.S., by initiating similar prohibitions as those used in Executive Order 13873. Within the order, the Secretary of Energy (Secretary) is empowered to prohibit the acquisition, transfer, or installation of certain BPS electric equipment, sourced from foreign adversary countries for one year.

On December 17, 2020, the Secretary issued the December 2020 Prohibition Order, which took effect January 16, 2021, under the authority of Executive Order 13920. The Prohibition Order prevented a limited number of utilities from acquiring, transferring, or installing certain BPS electric equipment, subject to the jurisdiction of the People's Republic of China.

Executive Order 13984: Taking Additional Steps To Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities

Order 13984, issued January 19, 2021, amends Executive Order 13694 released April 1, 2015. The order addresses additional steps needed to deal with activities conducted by foreign actors, to harm the U.S. economy through theft of intellectual property and sensitive data, and to target U.S. critical infrastructure through malicious cyber actions.

The order notes that malicious use of Infrastructure as a Service (IaaS) products and services (e.g., processing, storage, and computing resources) by cyber actors threatens the U.S. economy, national security, and critical infrastructure through the theft of intellectual property and sensitive data. Foreign actors employ U.S. IaaS products to impede tracking and evidence collection. Foreign resellers of U.S. IaaS exacerbate the problem allowing less-sophisticated foreign actors to cheaply and anonymously access these products, initiate cyber attacks, and evade detection and prosecution since no identification was previously required to open such accounts.

Order 13984 provided the authority to impose record-keeping requirements for foreign transactions. To address these threats, and to deter foreign malicious cyber actors use of U.S. IaaS products, and to assist in the investigation of transactions involving foreign malicious cyber

actors, providers offering U.S. IaaS products are required to verify the identity of parties obtaining an IaaS account for the provision of these products and maintain records of those transactions.

Executive Order 13990: Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis

On January 20, 2021, Executive Order 13990 was issued addressing a wide range of issues including environmental policy. It also suspended Executive Order 13920 for 90 days to allow the Secretary of Energy and the Director of the Office of Management and Budget (OMB) to jointly consider whether to recommend a replacement order be issued to revoke the December 2020 Prohibition Order, preventing the acquisition, importation, transferal, or installation of select BPS electric equipment manufactured or supplied by the People's Republic of China. The Department of Energy revoked the 2020 Prohibition Order as of April 20, 2021 "to create a stable policy environment before the emergency declaration made by Executive Order 13920 expired on May 1, 2021," and the Department conducted a Request for Information to "develop a strengthened administrable strategy to address the security of the U.S. energy sector."

Responses to the Request for Information by the electric industry highlighted the effective, extensive, and expensive set of existing cybersecurity tools, processes, and regulatory requirements that already protect electric utilities. The responses urged that future purchasing restrictions be based upon careful risk-based analysis and warned against potentially duplicative requirements. Utility comments also requested clear and specific information regarding future component prohibitions that will not place undue burdens on utility purchasing efforts.

Executive Order 14028: Presidential Executive Order on Improving the Nation's Cybersecurity

On May 12, 2021, the White House issued Executive Order 14028 addressing concerns about cybersecurity protections for federal agencies. The order directs the federal government to partner with the private sector to increase efforts to protect against attacks involving supply chain vulnerabilities. It orders the Department of Energy to develop recommended guidelines for requiring suppliers to federal agencies to provide SBOM information. Such source information on both software and hardware provides traceability for detecting and thwarting the use of malware. Though these DOE guidelines apply only to federal agencies, the effort was intended to set in motion broader efforts for use of SBOMs across all critical infrastructure sectors.

The order also directs responsible agencies to improve their capabilities for detecting intrusions and remediation of control deficiencies. For example, it establishes a Cyber Safety Review Board to review and assess major incidents in cooperation with the Department of Homeland Security. Following a cyber incident, when deemed necessary, the Board is to establish a Cyber Unified Coordination Group to assess the need for improved cybersecurity and incident response practices.

White House Memorandum, July 28, 2021

On July 28, 2021, the White House issued a Memorandum regarding cybersecurity for industrial control systems operating within critical infrastructure environments. The memorandum established the Industrial Control Systems Cybersecurity Initiative, a collaborative effort between the Federal Government and the critical infrastructure community, to "significantly

improve the cybersecurity of ICS," by deploying technologies providing threat visibility, indications, detection, warnings, and response capabilities. The initiative began with a pilot effort within the electric subsector, and is to be followed by a similar effort for the natural gas sector. The Memorandum states that similar efforts for the water and wastewater sectors will begin later this year.

The Memorandum also announced a new Department of Homeland Security effort to develop and issue cybersecurity performance goals for critical infrastructure. These performance goals will establish a common understanding of baseline security practices for critical infrastructure owners and operators.

The Department of Homeland Security and Department of Commerce, in collaboration with other agencies developed preliminary goals for control systems across critical infrastructure sectors in September 2021. These goals will be followed by issuance of sector-specific critical infrastructure cybersecurity performance goals by July 2022.

2.6.2 Federal Legislation

Between April and June 2021, the U.S. House Energy and Commerce Committee referred several House Resolutions to the U.S. Senate proposing enhancements to the Bulk Electric System's security and resiliency. These resolutions proposed specific duties and authority for the Department of Energy, CISA, and the Department of Homeland Security.

On November 15, 2021, H.R. 3684 *Infrastructure Investment and Jobs Act* was signed into law. The bill's provisions overlap with many of the electric utility sector protection enhancements proposed in the various House Resolutions that are pending Senate review.

Selected provisions of H.R. 3684 that relate to the security and resiliency of the BES are displayed in **Appendix 1.** Allocation of authorized funds, programs, and specific expenditures among the various U.S. critical infrastructure sectors is to be determined. Roles of the various federal agencies are not known, nor is the future impact of these authorized investments and expenditures on Florida electric utilities.

2.6.3 Federal Energy Regulatory Commission Action

On December 17, 2020, the Federal Energy Regulatory Commission issued a Notice of Proposed Rulemaking (NOPR), pursuant to sections 205 and 206 of the Federal Power Act, that proposes incentives for certain cybersecurity investments that go above and beyond the requirements of NERC.

The proposed cybersecurity incentives framework would encourage public utilities to undertake cybersecurity investments on a voluntary basis to better ensure secure service for ratepayers. This approach would incent a public utility to adopt cybersecurity practices that would not only better protect its own systems but also improve the cybersecurity of the Bulk-Power System.

The NOPR includes two proposed incentive approaches. Under one approach, a public utility may receive incentive rate treatment for voluntarily applying identified CIP Reliability Standards to facilities that are not currently subject to those requirements.

Under a second option, a public utility may receive incentive rate treatment for implementing certain security controls included in the NIST Cybersecurity Framework.

Under the NOPR, a public utility planning cybersecurity investments consistent with the two approaches described above would be eligible for either of two incentive rewards: either a 200 basis-point add-on to the return on equity applied to the eligible cybersecurity capital investments or deferred cost recovery for certain expenses related to the cybersecurity investments.

2.7 Cooperative Resources for Cybersecurity Protection

The utilities maintain an around-the-clock incident response team of cybersecurity personnel and coordinate with national labs, government agencies, industry partners, vendors and law enforcement officials to best protect its energy grid and IT and OT systems. The sharing and receiving of cybersecurity intelligence is augmented from the following key organizations:

- The Department of Energy's (DOE) Cybersecurity Risk Information Sharing Program (CRISP) is a public-private data sharing and analysis platform that facilitates the timely sharing of cybersecurity threat information among energy sector stakeholders. NERC recently partnered with CRISP to include two new OT pilot programs. The purpose of these programs is to identify potential cyber threats to ICS by capturing OT data and comparing it to CRISP IT data.

- 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, who are able to provide voluntary assistance to each other in advance of a cyber emergency that disrupts electric or natural gas services.

- The Electricity Information Sharing and Analysis Center (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 Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) provides alerts intended to provide timely information about current security issues, vulnerabilities, and exploits.

- 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. The NSA recently issued a cybersecurity advisory that included a list of recommended best practices to stop malicious cyber activity against IT/OT connected networks.

- 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-13 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. For example, EPRI released the results of an electromagnetic pulse (EMP) study in April 2019. EPRI concluded that the potential effects of initial and late pulses from an EMP event could trigger a regional service interruption with minimal damage to large power transformers. It believes this interruption would not trigger a nationwide grid failure. Recovery times would be expected to be similar to other major interruptions upon execution of appropriate mitigation efforts. EPRI is collaboratively working with utilities to further evaluate mitigation options. EPRI also recently prioritized five emerging OT/ICS cybersecurity topics: 1) automating cybersecurity capabilities, 2) supply chain risks for procurement and installed equipment, 3) quantifiable data to support risk model and decision-making; 4) cloud security for real-time systems, and 5) cybersecurity for DERs.

3.0 NERC Compliance Standards

3.1 NERC CIP Reliability Standards

From 2008 to date, FERC has approved 13 CIP reliability standards to protect the BES from cyber and physical attacks. Each CIP standard is broken down into cyber and physical security protection requirements. The requirements include 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-privileged, 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 factors 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.

NERC employs a consistent 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 2** provides a list of the 12 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 CIP-002 through CIP-009 reliability standards 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 2021			
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	6	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	3	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-013	1	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	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 2

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. For example, CIP-005 now requires system owners and

operators to log and monitor vendor remote access when procuring industrial control system hardware, software, and other networking services.

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. Specific 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.

Also 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 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 mid-2022, final implementation of CIP-012 will impose security requirements regarding communications between control centers.

3.2 Emergency Preparedness and Operations Standards

Section 215 of the Federal Power Act required NERC to develop mandatory and enforceable Reliability Standards that are subject to FERC review and approval. 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-004-4 (Event Reporting) requires reportable physical security events (e.g., 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 to assure

reliability is maintained during restoration and priority is placed on restoring the interconnection.

- EOP-006-3 (System Restoration Coordination) requires 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-008-2 (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 operating plans to mitigate operating emergencies, and that those plans are coordinated 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 a specific set of reliability 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 Geomagnetic Disturbance (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. This standard addresses risks of voltage collapse and equipment damage in the BES caused by GMD events. 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 Duke Energy Florida, LLC

Duke Energy Corporation (Duke Energy) supplies energy to about 7.7 million U.S. retail electric customers in the Carolinas, Midwest, and Florida. Duke Energy Florida (DEF), a subsidiary of Duke Energy operates 166 transmission and 232 non-BES transmission substations, providing about 10,200 megawatts of owned electric capacity to more than 1.8 million retail customers in Florida.

4.1 Cybersecurity Management Oversight

The cybersecurity program at Duke Energy leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework to manage cyber and physical security risks. The following core strategies are the foundation of the 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.

To oversee the cyber and physical security practices throughout the company's six regulated utilities, Duke Energy created its Enterprise Security Compliance Model. The model consists of executives and business units responsible for managing and maintaining focus on NERC compliance, as well as a governing set of policies and procedures.

The company employs detailed cybersecurity reporting requirements and policies defining the roles, responsibilities, and the processes for identifying, evaluating, and mitigating suspected cyber security incidents. The policies apply to a cyber incident on any Duke Energy system (IT and OT) and any third-party system impacts to Duke Energy's business operations or delivery of energy services.

4.1.1 Compliance Reorganization

Since 2017, Duke Energy has sought to improve communication between management levels within Duke Energy's regulated utilities and its corporate cybersecurity organization. Previously, Duke Energy's various business units were each responsible for maintaining CIP compliance within their operations. Additionally, Duke Energy's cyber and physical security organizations were treated as separate entities resulting in the security functions operating independently with

limited collaboration on enterprise-wide risk. This created the risk of organizational silos across business units and potential confusion regarding expectations and responsibilities.

Duke Energy recognized the need to shift its management culture to raise the bar for its CIP compliance efforts and program documents, oversight and training. A centralized CIP Program Management (CPM) department with compliance oversight was created to provide for a clearer chain of command. Changes include converged cyber and physical security functions, restructured roles, updated systems to better track access and vulnerabilities, and additional resources to help manage and implement compliance and security efforts.

Exhibit 3 depicts Duke Energy's restructured Enterprise Security NERC Oversight Compliance Model. The Senior Vice President-Chief Security Officer (CSO) oversees Duke Energy's cyber and physical security and has overall authority and responsibility for ensuring ongoing adherence to CIP standards. The CSO provides cybersecurity updates monthly to the Electric Reliability Executive Steering Committee, quarterly to Corporate Audit Services, and annually to the full Board of Directors. Updates include the status of CIP compliance corrective measures, cybersecurity performance metrics results, and risk analyses.

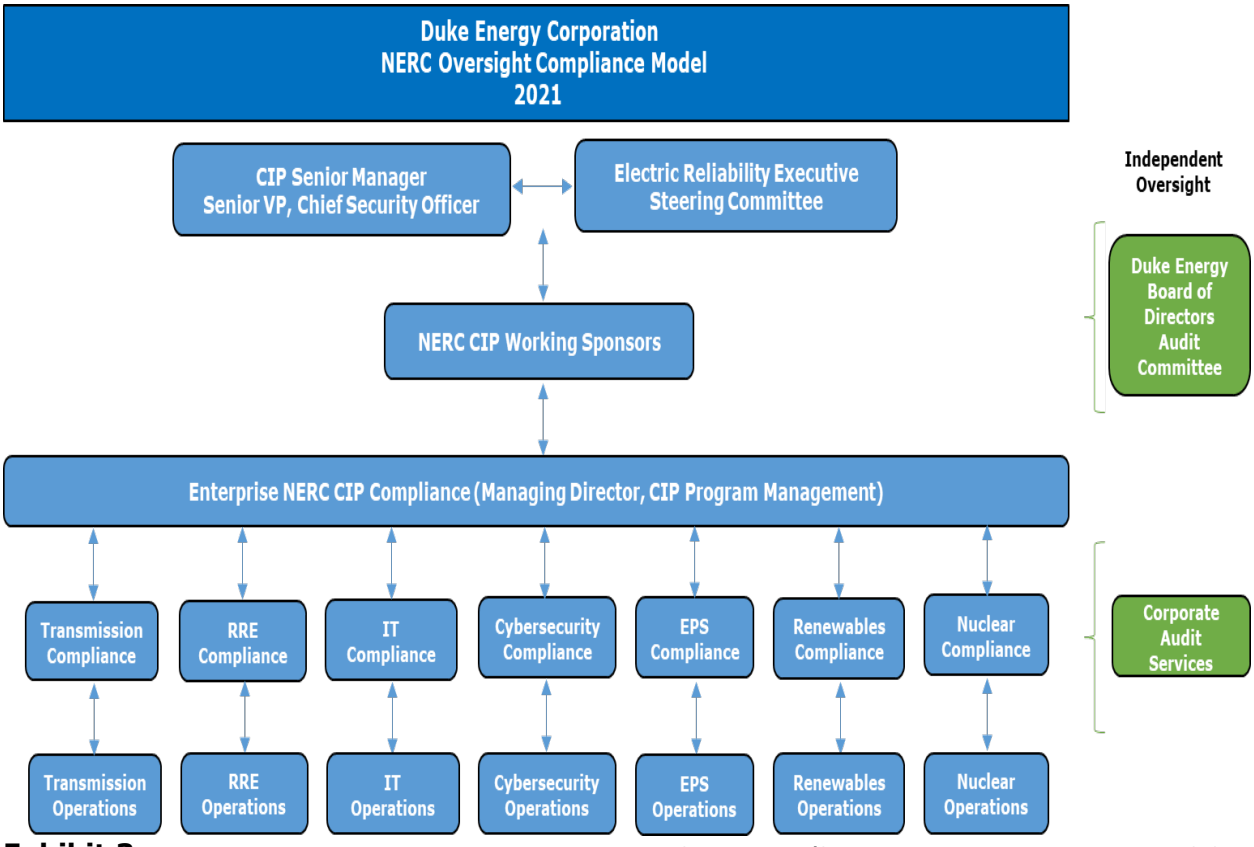

Exhibit 3

Source: DEF'S Response to Document Request 2.2

Under the direction of the CSO, the NERC CIP Working Sponsors are comprised of directors and managers from the eight business units responsible for maintaining focus on NERC compliance.

To further strengthen NERC CIP compliance, Duke Energy enhanced the CIP Program Management (CPM) organization position. The CPM's responsibilities include performing quality assurance reviews, training, change management and validation of compliance with the company's IT 503 NERC CIP cybersecurity policy discussed below.

This new structure provides for clear lines of communication and accountability from the business unit leaders, allowing the CSO to direct the company's overall CIP program and strategies and adhere to compliance.

The company also operates centralized cyber and physical security centers to more effectively address threats and attacks. The Cybersecurity Operations Center operates 24x7 providing enterprise-wide cybersecurity monitoring. Using a platform of diverse tools and vendors, the center's personnel perform intrusion detection, prevention, and event management functions. The physical security of the company's facilities is overseen by the Enterprise Security Operations Command Center. This control center provides physical access video monitoring, intrusion detection, information reporting, and security support services. In 2022, a planned new cyber center will be tasked with monitoring, detecting, analyzing, and responding to cybersecurity incidents occurring in the OT environment.

According to Duke Energy, the company has achieved overall improvement in CIP compliance, security practices, management oversight, and collaboration between cyber and physical security functions. Duke Energy believes that as a result of recent program improvements, it can more effectively identify and mitigate threats.

4.1.2 Policies and Procedures Updates

As described in **Exhibit 4**, Duke Energy's IT 500 Policy Stack, includes cybersecurity standards, processes, procedures, templates, and best practices. Beginning 2021, Duke Energy revised and re-categorized its IT 500 Policy stack to better align them with the NIST Cybersecurity Framework and to more effectively manage the company's cyber and physical security practices. Changes included revised and new processes, internal controls, and training protocols. According to Duke, these efforts have resulted in more clearly defined guidelines and expectations.

Subsumed within the updated IT 503 policy are the multiple IT cybersecurity standards that establish compliance requirements for NERC reliability standards CIP-002 through CIP-014. This alignment clarified expectations for CIP compliance. Improvement efforts were also aimed at program documents, training, internal controls, and management oversight that had been intended to identify and prevent the deficiencies.

Duke Energy Corporation IT 500 Policy Stack 2021	
Standard	**Purpose**
IT 501 Cybersecurity Standard	Contains controls for continuous monitoring on non-NERC CIP IT assets.
IT 502 Industrial Control Systems	Provides requirements for specifying the security controls for organizations and information that support ICS used within distribution control center and non-BES substations.
IT 503 NERC CIP Cybersecurity	Governing document that establishes responsibility and management controls to comply with the NERC CIP Standards.
IT 504 Smart Grid	Contains controls to address the unique risks associated with new smart grid technologies and grid modernization systems.
IT 505 Third Party Service Provider	Contains controls for protecting against risks associated with third party service providers.

Exhibit 4 *Source: DEF's Response to Document Request 1.2*

4.2 Audits and Self-Assessments

4.2.1 CIP Compliance Audits

SERC performs periodic NERC CIP compliance audits, providing a rigorous, systematic, and objective examination of CIP compliance-related records and activities. The 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 taken are documented to ensure compliance.

Between 2016 and 2021, SERC performed one comprehensive audit and three narrower scope audits of Duke Energy's compliance with CIP standards. Resolution of all findings and remedial actions is complete or nearing completion for these audits.

4.2.2 Self-Assessments

NERC also relies on Duke Energy to convey non-compliance issues through a mandatory self-reporting process. The company uses an internal compliance tracking tool to track potential violations and mitigation plans that include corrective actions to reduce the likelihood of a future occurrence. Utilities such as DEF identify and self-report compliance deficiencies as they are discovered. As part of the NERC Compliance Monitoring and Enforcement process, SERC reviews and takes into consideration the self-reported non-compliance issues in developing findings, approving corrective action, and imposing penalties. Where applicable, Duke Energy has taken action on self-reported deficiencies, including restructuring oversight responsibilities and processes and revising procedures.

Duke Energy also evaluates enterprise cybersecurity capabilities using the Department of Energy's Capability Maturity Model (C2M2). The C2M2 is a voluntary evaluation tool for assessing the degree of cybersecurity program growth and development. It is also used to

prioritize cybersecurity actions and investments. C2M2 allows a utility to identify gaps in security capability, prioritize those gaps and develop plans to address them.

Duke Energy completed its most recent C2M2 assessment in November 2018. The results were used as inputs into Duke Energy's 2019 cybersecurity Strength, Weakness, Opportunity, and Threat (SWOT) analysis. The SWOT analysis helps the company identify the current status of risks and set priorities to improve defenses.

Duke Energy Corporate Audit Services performs internal audits to assess the adequacy of cyber and physical security internal controls. Over the period 2019 through 2021, Audit Services has conducted several audits covering specific security-related issues with remediation of any findings either ongoing or completed.

4.3 Risk Management

4.3.1 Risk Registers

In executing the NIST Cybersecurity Framework's core functions (identify, protect, detect, respond, and recover) Duke Energy employs its Enterprise Security Risk Register. Mitigation response actions are documented on the DEF Enterprise Security Risk Register. The risk register documents the results of risk-based analyses used to identify and rank specific risks and trends. The analysis includes estimates of probability of occurrence and likely extent of potential harm. For each identified risk, the company develops targeted mitigation strategies. Ongoing tracking allows DEF to monitor and update the risks and mitigation plans as the threat environment evolves.

Management teams within each of the company's business units shown in **Exhibit 3** are responsible for identifying, assessing, and maintaining cybersecurity risk registers. Each business unit director performs monthly reviews with the company's senior leadership of the risks and associated actions. In turn, the senior leadership, including the Chief Security Officer (CSO) and the Chief Risk Officer (CRO), conduct quarterly risk reviews with the company's Enterprise Risk Management (ERM) team. Both the CSO and CRO are responsible for sharing key company risk information with the Board of Directors. The ERM team prioritizes the risks within each business unit's risk register through the use of probability and impact criteria.

4.3.2 Metrics

Cybersecurity risks can also be addressed through tailored cybersecurity metrics used as quantified performance indicators. These metrics are targeted performance indicators that provide comparable quantitative measurement. Duke Energy employs a metrics program to identify critical infrastructure vulnerabilities and to ensure appropriate security protections are in place. Metric performance that indicates off-target results will trigger investigation and corrective action. The company presently reports over 40 physical and cybersecurity metrics. Key metrics include:

- Patching status of vulnerabilities
- Aging of unpatched vulnerabilities

- Click rate against "real" phishing emails
- Average detect-to-response time against cyber threats
- Camera inoperability rates
- Alarm rates
- Non-HR badge issuance
- Business Continuity Plan evaluation
- Background Investigation turn-around time

Duke Energy actively participates in an Electric Power Research Institute (EPRI) research project to develop cybersecurity performance metrics. EPRI offers a web-based platform, or metrics hub, which is available for use by utilities. The platform supports automated cyber security data collection, security metrics calculation, visualization, and analysis. These metrics can be applied to both IT and OT security environments.

4.4 Cybersecurity Protection Trends and Issues

4.4.1 Convergence of IT and OT

Across the utility industry, the trend of convergence of IT/OT networks and the increased deployment of distributed energy resources (DERs)[4] both increase OT system vulnerabilities to cyber attack. Other contributing factors are IT/OT system reliance on hardware and software procured from a number of different manufacturers and vendors around the globe.

Duke Energy continues to converge its IT/OT networks and deploy smart grid devices to enhance system reliability and resiliency. The network convergence and use of smart grid devices allow for increased operational efficiencies such as automatically detecting outages and rerouting power to restore service quicker or avoiding the outage altogether.

Other benefits include improved data collection on the performance of customer-owned DER equipment connected to DEF's distribution grid. As DERs expand and become more aggregated, managing and securing the two-way energy flow systems becomes more complex. The industry is working to further develop cybersecurity protections for the growing deployment of DERs to reduce vulnerabilities.

Duke Energy continues to work on grid security improvement initiatives such as an ongoing Cybersecurity IT-OT Program at a cost of $137.4 million in capital investments. The program is intended to enhance hardware and software for automated asset identification and management, intrusion protection and detection, and attack response and recovery hardware. Duke maintains OT asset tracking through a variety of systems depending on criticality of the equipment. These inventories are periodically verified through walk down reviews and updated accordingly.

Duke Energy also employs network segmentation to create separate areas on the network, rejecting unnecessary traffic, to mitigate the harm of malware by isolating it to a limited part of

[4] In 2020, DEF had 34,111 renewable generation customers, up 60.3 percent from 21,277 customers in 2019. Data at: http://www.floridapsc.com/ElectricNaturalGas/CustomerOwnedRenewableEnergy

the network. Duke Energy's OT environment is designed with the ability to isolate from the IT environment to maintain OT core functionality.

4.4.2 Supply Chain and Cloud Services Protections

According to NERC's August 2021 Reliability Report, supply chain cybersecurity incidents in North America increased 118% from 2019 to 2020. Since the public announcement of the Solar Winds attack, all utilities using SolarWinds software were prompted to search systems for evidence of malware intrusion. Most utilities redoubled efforts to ensure full compliance with NERC's CIP-013 standard.

Duke Energy's Cyber Incident Response Team (CIRT) initiated an investigation and determined that operations were not impacted or compromised. Duke Energy continues to work closely with industry partners to execute upgrades and countermeasures as they become available. Duke Energy conducts assessments on third-party vendors and has updated its IT-503 supply chain standards to reflect current requirements and added additional protections into its contracts with third-party vendors.

To explore the use of SBOMs to protect against malware attacks, Duke Energy is participating in an Energy Sector SBOM Proof of Concept Team sponsored by the National Telecommunications and Information Administration and the Department of Energy. Early indications from the team show that suppliers are not ready to provide SBOMs for their software and also that the utility industry may need to develop tools and processes to facilitate the use of SBOMs.

The process of tracking and updating component sources would involve substantial cost increases to vendors and their utility customers. The process of maximizing the potential benefits of SBOMs may be lengthy. According to Duke Energy, regulatory actions such as Executive Order 14028, issued in May 2021, may speed future adoption of SBOM standards and requirements in the electric utility industry. It should be noted that Duke has updated its vendor contracts to include additional software security requirements to enhance supply chain integrity.

Duke Energy uses cloud computing to obtain additional computer system resources such as storage space and network bandwidth, and applications. Duke Energy has a formal governance structure for managing all aspects of cloud deployment, usage, operations, and security. Controls in place to protect against cloud service compromise include but are not limited to limiting network and data exposure, monitoring of traffic to and from the cloud service providers, detecting anomalies, and providing blocking functions.

4.4.3 Distribution Protections

A report by the U.S. Government Accountability Office on electric distribution system cybersecurity concludes that:

> The grid's distribution systems, which carry to consumers the electricity essential to modern life, are increasingly at risk from cyber attacks. DOE, DHS, and other federal agencies have provided resources to states and industry to help them improve the cybersecurity of distribution systems. However, DOE's plans for implementing the national cybersecurity strategy for the grid do not fully address risks to these systems. While a cyberattack on distribution systems may

be less significant than one on the bulk power system, the impacts of such an attack could still result in outages of national significance. Unless DOE more fully addresses risks to the grid's distribution systems in its updated plans, federal support intended to help states and industry improve distribution systems' cybersecurity will likely not be effectively prioritized.

As previously noted in this report, DERs may increasingly introduce risks to utility distribution grids. In response to DER risks, Duke Energy is actively participating with DOE in its Grid Modernization Laboratory Consortium (GMLC) Resilient Distribution System Project that includes the treatment of DERs. The objective of the GMLC project is to anticipate and recover from grid events by demonstrating predictive analytics capabilities. Successful completion of this project will allow DEF to maintain secure interoperability and real-time distributed intelligence. The company also participates in research with EPRI, IEEE, and NIST to tackle DER cybersecurity challenges.

4.5 Response and Recovery

4.5.1 Participation in Drills and Exercises

Duke Energy's CIRT performs multiple response drills across its business units and participates voluntary programs in coordination with federal, state, or local emergency authorities. Drills and programs range from malware detection, tabletop exercises to activating command and control structures.

Duke Energy participates biennially in NERC's GridEx, the nation-wide operational exercise a biennial North American grid security exercise sponsored and hosted by NERC. GridEx tests emergency response and recovery plans in response to simulated cyber and physical security attacks and other contingencies. Duke Energy and its operating utilities participated in GridEx VI in November 2021. The GridEx VI objectives were 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.

Duke Energy states that it performs cyber threat hunting activities and internal and external penetration testing on its environment throughout the year. Threat hunting is a defense activity involving iterative searching of networks to detect and isolate advanced threats that have evaded existing protections. Penetration tests are authorized cyber attacks intended to identify weaknesses or vulnerabilities in systems, networks, human resources, or physical assets.

4.5.2 Incident Reporting and Response Planning

Effective January 1, 2021, NERC CIP-008 requires entities to report cybersecurity incidents that compromise, or *attempt* to compromise. According to DEF, the determination of an *attempt* to compromise is based on evidence observed from threat actors targeting electronic and/or physical security perimeters that impact high and medium BES cyber systems.

NERC EOP-004 requires responsible entities to report physical security events that threaten the reliability of the BES. Events are to be recorded and submitted to NERC, SERC, Department of Energy, law enforcement, and other government authorities.

For the period 2018 to date, Duke Energy states that it has not experienced any cyber or physical security incidents requiring reporting and response pursuant to the NERC requirements. The roles, responsibilities, and processes for problem source identification, mitigation, and eradication triggered by a suspected cybersecurity incident are defined in Duke Energy's IT-503 Policy Stack. Duke Energy also requires its cybersecurity incident response process to be tested annually.

4.5.3 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.

Duke Energy has implemented the restoration plans required by EOP-005 addressing detailed strategies and priorities for restoration. These plans address coordination with the reliability coordinator, procedures for restoring interconnections with other transmission operators, and processes to restore loads for system restoration.

EOP-008 requires focus on maintaining reliable operations of the BES in the event that primary control center functionality is lost. Duke Energy has implemented a documented plan containing, 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.

Duke Energy states that it has implemented the operating plans required by EOP-011, including the processes and procedures to prepare for and mitigate operating emergency situations.

5.0 Tampa Electric Company

Tampa Electric Company (TEC), and its parent TECO Energy, Inc., are wholly-owned subsidiaries of Emera Incorporated of Halifax, Nova Scotia. TEC serves approximately 800,000 residential, commercial, and industrial customers in a 2,000 square-mile service area within Hillsborough, Polk, Pasco, and Pinellas counties. The company operates more than 5,000 megawatts of generating capacity, with 226 substations, including 82 transmission substations and 144 distribution substations.

5.1 Cybersecurity Management Oversight

In 2019, Emera began to align its cybersecurity standards with the National Institute of Standards & Technology (NIST) Cybersecurity Framework. TEC's IT cybersecurity organization was reorganized in 2020 to make Enterprise Information Security more policy- and risk-management focused. All operational aspects of cybersecurity were distributed into the centralized IT operational group. The IT operating model transformation sought to encourage a culture of security within IT and to make cybersecurity operations more responsive and effective.

In June 2021, TEC opened a new Physical Security Operations Center at the Ybor Data Center. It is co-located with TEC's Cybersecurity Operations Center to promote improved collaboration and information sharing between physical security and cybersecurity.

5.1.1 Management Oversight Structure

Exhibit 5 displays the organizational structure of TEC work units responsible for cybersecurity protection. TEC's Vice President of Information Technology & Chief Information Officer is the company's designated CIP Senior Manager and is responsible for managing NERC CIP compliance. The IT department provides technical support to all departments responsible for CIP requirements.

The Director of Technology Delivery, Performance Optimization & Compliance chairs the CIP Steering Committee that coordinates CIP compliance activities across all departments. The Director Strategy, Security, and Governance is responsible for Information Security, and for establishing cybersecurity objectives, strategies, and programs. The Director ensures that all IT and OT cyber systems, assets, and networks are aligned with the Emera cybersecurity framework.

TEC's Vice President of Regulatory Affairs & Business Strategy oversees NERC compliance audit interactions and directs communications with FERC and SERC. Support for these functions is provided by the Director Federal Regulatory Affairs, Compliance, and Transmission Policy and the Manager of FERC Compliance.

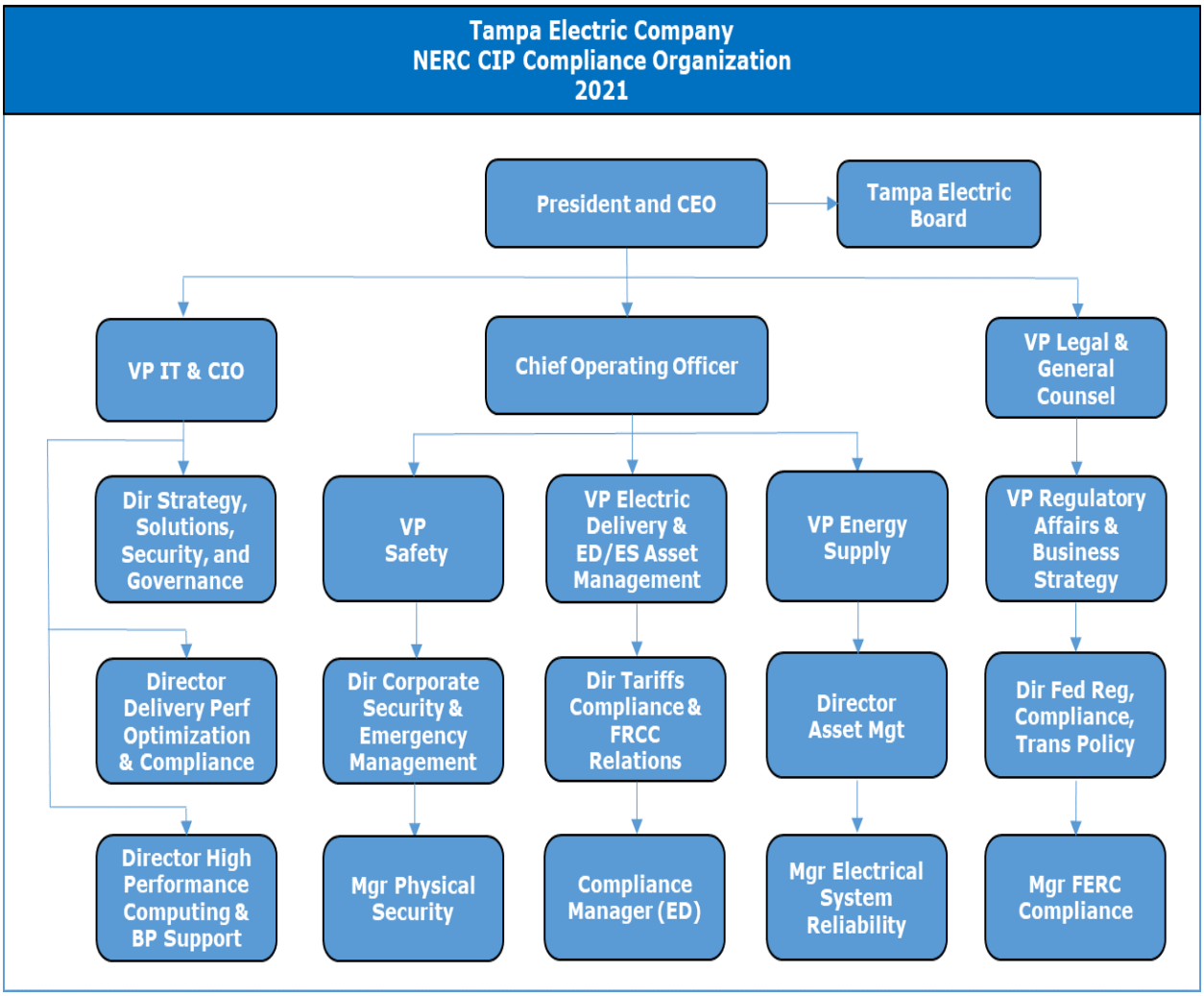

Exhibit 5 *Source: Document Request 3.89*

5.1.2 Policies and Procedures Updates

Emera has developed a set of Policies and Standards, based on the NIST Cybersecurity Framework, and plans to potentially adopt them within Emera's subsidiaries and affiliates during the period 2021-2024. These standards cover areas of operations, protection of critical assets, conduct of employees, and the priority of regulatory compliance.

TEC's Information Security Policy is based on the Emera Cybersecurity Policy which provides the uniform governance and security-controls baseline for Emera affiliates. TEC's Asset Management Standard and related security policies and plans require identification of all IT and OT critical facilities and/or cyber assets. The Asset Management Standard details controls for IT and OT asset inventory, including responsibilities for assets, information owners, and asset disposition processes.

5.2 Audits and Self-Assessments

5.2.1 CIP Compliance Audits

SERC Reliability Corporation is the Regional Entity responsible for monitoring and auditing TEC's compliance with NERC CIP Standards. SERC's most recent audit of TEC's NERC CIP compliance was completed in May 2020. The scope included selected requirements from CIP-002, CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and CIP-011. Audit response activities have been approved by SERC and process improvements have been completed.

5.2.2 Self-Assessments

In the course of operations, utilities occasionally identify CIP compliance deficiencies or potential issues. In these cases TEC is required to self-report the deficiency to SERC. Any corrective action needed may be addressed in the next SERC audit. The company notifies SERC, describes the condition observed, submits a mitigation plan, and implements mitigation actions upon approval by SERC.

In June 2018, TEC performed a voluntary self-evaluation using the Department of Energy's Cybersecurity Capability Maturity Model. Based on prior use of the model and this most recent evaluation, TEC management believes the C2M2 process is valuable in prioritizing needs and targeting efforts at program development. Another C2M2 self-evaluation may take place in 2023.

Internal audit functions at both the Emera corporate and TEC subsidiary levels provide analyses of cybersecurity internal control adequacy. Over the period 2018 through 2021, Emera has performed assessments of TEC's degree of implementation of corporate cybersecurity standards and other readiness and protection adequacy reviews.

5.3 Risk Management

5.3.1 Risk Registers

If elements of the Cybersecurity Framework or related information security standards cannot be met, an exception is filed by the appropriate team and if approved by the designated bodies will be tracked by IT Compliance until it is remediated. Security assessments, vulnerability assessments, and penetration tests follow the same process for any findings that cannot be remediated or mitigated in a reasonable timeframe. This exceptions list serves as TEC's risk register.

A risk register of all vendors is maintained, reviewed, and updated. As TEC implements a third-party risk management tool and vendor contracts are renewed or new vendors are added, each vendor is reviewed through the tool and a risk register is created for that vendor. The risk management tool ensures that parties do not create an unacceptable potential for business disruption or cybersecurity risk in TEC's supply chain.

5.3.2 Metrics

TEC actively participates in an Electric Power Research Institute (EPRI) research project to develop cybersecurity performance metrics. EPRI offers a web-based platform, or metrics hub,

which is available for use by utilities. The platform supports automated cybersecurity data collection, security metrics calculation, visualization, and analysis. These metrics can be applied to both IT and OT security environments.

5.4 Cybersecurity Protection Trends and Issues

5.4.1 Convergence of IT and OT

IT/OT convergence is the integration of information technology systems with operational technology systems. TEC defines Information Technology as systems with a focus on business and enterprise systems that store, process and deliver information. Operational Technology is systems that manage, monitor and control industrial operations with a focus on the physical devices. From a security perspective, OT mainly involves protecting physical processes, safety, production, efficiency and protection of employees. IT security is directed at protecting all aspects of data and how information is stored, transmitted, processed, and used in business processes.

For NERC-related IT or OT hardware, software, and services, there are specific requirements within the CIP-013 Cybersecurity Supply Chain Risk Management standard for a risk management plan; within CIP-005 for vendor remote access and within CIP-010 for software integrity and authenticity. CIP-013 and associated changes for CIP-005 and CIP-010 for Supply Chain Risk Management were implemented by TEC by the compliance effective date of October 1, 2020. Third-party personnel with IT and/or OT responsibilities are required to take the NERC CIP Access annual training course for non-employees as a prerequisite for electronic access or unescorted physical access to High or Medium Impact BES cyber systems.

5.4.2 Supply Chain and Cloud Services Protections

TEC's Outsourcing, Vendor Management & Cloud Management Standard guides the assessment of supply-chain cybersecurity risk for each vendor. Prior to outsourcing any IT function or data storage, the information security capabilities of the proposed third-party service providers must be assessed. Vendor and cloud-based risk assessments are also being integrated into new projects and vendor engagement processes.

During 2020, TEC enhanced its supply chain risk management program in several areas. Through the NERC CIP-013 Implementation project, procurement processes were updated for greater inclusion of the Enterprise Information Security team in the procurement lifecycle for evaluation of cyber risk associated with potential suppliers. TEC's updated contract terms and conditions include additional language around cyber risk management and related vendor responsibilities such as reporting a cybersecurity event to TEC.

To improve the Enterprise Information Security team's capabilities in assessing vendor risk, Tampa Electric purchased an integrated product solution in quarter one 2021. The solution combined point-in-time and continuous cyber risk intelligence scoring with software workflow-based vendor risk questionnaire system that queries vendors on their cyber hygiene using the industry recognized Standardized Information Gathering questionnaire.

Regarding the Solar Winds supply chain attack, TEC determined that the version in use on TEC's network was a clean, non-compromised version. Out of an abundance of caution, the SolarWinds environment was rebuilt using the vendor verified non-compromised version.

In response to Executive Order 13920, the NERC alert Supply Chain Risk III, and the Prohibition Order Securing Critical Defense Facilities, TEC took steps to review pertinent vendor equipment manufactured or purchased from third-party service providers and found no potential risks present via products from enemy states of the U.S. TEC is also monitoring Executive Order 14028 for further guidance on the development of SBOMs and will implement any resulting federal agency requirements.

TEC benefits from using cloud-based services for cybersecurity such as multi-factor authentication, data loss protection, email domain-based message authentication, reporting and conformance, and distributed denial-of-service protection. These cloud-based services are engineered by companies specializing in specific IT areas. However, TEC does not use cloud-based services for OT applications. Not having responsibility for infrastructure and platform greatly simplifies the operations on the business side.

TEC cloud-based services can pose physical and cyber-related risks, but the company notes such risks are not unique to cloud environments and have always been present within any IT security landscape. TEC's cloud-based service providers maintain controls to mitigate or remediate those risks before they reach the data center and services they provide. Vendor and cloud-based risk assessments are being integrated into vendor engagement processes including use of the third-party risk management tool.

5.4.3 Distribution Protections

The electric utility industry realizes that increasing distribution system remote access and connections to business networks can enlarge the threat surface exposed to cyber attack. TEC believes the residual risks to its distribution control systems are reduced to an acceptable level by using the same basic security architecture to protect distribution and industrial control systems as it uses to protect BES assets.

Though TEC has not experienced any threat actions that indicate its distribution or industrial control systems are more vulnerable or endangered, the company does recognize the unique cyber and physical security risks and protection challenges DERs present. DERs differ from central generation resources in that they are geographically distributed, typically smaller capacities, scalable, often unmanned, and may be interconnected at transmission and distribution voltages. These characteristics make cost-effective protections challenging.

These challenges depend also on whether the DER is under the control of TEC, customers, or third parties. Obviously, TEC is not able to mitigate physical or cybersecurity threats to behind-the-meter rooftop solar installations controlled by the owners of the systems. The small size of each system tends to limit the potential impact of an attack on individual systems. However, the risk of wide-scale cyber attacks increases as more of these systems are connected to the Internet.

5.5 Response and Recovery

5.5.1 Participation in Drills and Exercises

TEC follows an all-hazards approach to incident management and uses its Incident Command System as the foundational structure for incident response. To support incident response plan testing, TEC has a Comprehensive Exercise Program (CEP) that is used to plan for, practice, and measure the effectiveness of incident response plans through a variety of drills and exercises. The CEP is updated annually and includes a progressive, multi-year cycle for planning and execution of increasingly complex trainings and exercises. In addition, training and exercises align with NERC CIP standards and other physical security protective measures, including U.S. Coast Guard Maritime Security.

On a biennial basis, TEC participates in NERC's GridEx cyber and physical security exercises. In alternate years TEC conducts a separate exercise to test and validate its cyber and physical security plans. TEC conducts quarterly recovery tests of IT and some OT applications. In addition, physical security drills are conducted on a quarterly basis at various company locations.

As shown in **Exhibit 6**, TEC expects to participate in the following six exercises over the period 2022 through 2024.

Tampa Electric Company
Physical and Cybersecurity Exercises
2022-2024

Date	Exercise	Threat Scenario
Q2 2022	Privacy Breach	Cyber
Q4 2022	NERC CIP-008 – Incident Reporting & Response Planning	Cyber
Q2 2023	Cyber Shock Wave 3	Cyber
2023	Corporate Physical Security	Physical
11/2023	NERC Grid Ex VII (CIP-008 and CIP-003)	Cyber and Physical
Q4 2024	NERC CIP-008 – Incident Reporting and Response Planning	Cyber and Physical

Exhibit 6 *Source: Document Request Response 2.73*

TEC's Cybersecurity Operations Center (CSOC) monitors for unauthorized access, the introduction of malicious code, and any abnormal occurrences within the network. TEC's CSOC has an incident response program and playbooks to monitor, record, analyze, and respond to cyber security threats and incidents. TEC uses network intrusion detection software to monitor and detect known or suspected malicious communications that traverse the firewall.

TEC's CSOC developed a penetration testing program which began in 2020. These tests simulate external attacks on the TEC network, response to an assumed successful breach, and focused separate attacks on individual units. Penetration methods used include phishing, social engineering, and physical security intrusion simulation.

5.4.2 Incident Reporting and Response Planning

NERC CIP-008 requires entities to employ a process to identify, classify, and respond to emergencies, including cyber and physical security-related emergencies.

TEC uses various notification trees to ensure personnel make the required contacts in keeping with its notification protocols. TEC's protocols include notification requirements for the following agencies:

- Electricity Information Sharing and Analysis Center (E-ISAC)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Florida Reliability Coordinating Council (FRCC)
- Department of Energy (DOE)
- SERC Reliability Corporation
- Federal Bureau of Investigation (FBI)
- Local and state law enforcement

5.4.3 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. TEC also conducts quarterly IT and OT recovery tests.

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 neighboring utilities and the Florida Reliability Coordinating Council Reliability Coordinator.

Appendix 1
H.R. 3684 Infrastructure Investment and Jobs Act 2021

On November 15, 2021, the President signed into law H.R. 3684 *Infrastructure Investment and Jobs Act* that includes cybersecurity provisions for utility sector protection enhancements. Some notable provisions of the bill to enhance the security and resiliency of the BES are as follows:

Subtitle B – Cybersecurity

- **Enhancing grid security through public-private partnerships:** This section requires the Secretary, in consultation with State regulatory authorities, industry, NERC, and other relevant federal agencies, to carry out a program to promote and advance the physical security and cybersecurity of electric utilities, with priority provided to utilities with fewer resources. This section also requires a report to Congress on improving the cybersecurity of electricity distribution systems.

- **Energy Cyber Sense program:** This section establishes a voluntary Energy Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system.

- **Incentives for advanced cybersecurity technology investment:** This section directs FERC to initiate rulemaking to develop incentives that would encourage investment in cybersecurity technology and participation in cybersecurity threat information sharing programs.

- **Rural and municipal utility advanced cybersecurity grant and technological assistance program:** This section 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 to, and recover from cybersecurity threats. This section authorizes $250M for the period of FY22-26.

- **Enhanced grid security:** This section creates a program to develop advanced cybersecurity applications and technologies for the energy sector, a program to enhance and test emergency response capabilities of DOE, and a program to increase the functional preservation of electric grid operations or natural gas and oil operations in the face of threats and hazards. This section authorizes $250M for the period of FY22-26 for the Cybersecurity for the Energy Sector RD&D program, $50M for the period of FY22-26 for the Energy Sector Operational Support for Cyber resilience Program, and $50M for the period of FY22-26 for Modeling and Assessing Energy Infrastructure Risk.

- **Cyber Response and Recovery Fund:** This fund consists of $20M per year for 5 years (total of $100M). The provisions allow the Secretary of Homeland Security to declare a Significant Incident following a breach of public and private networks. The fund allows the CISA to provide direct support to public or private entities as they respond and

recover from significant cyber attacks and breaches. Any unused funds remain available until expended with the program ending September 30, 2028.

- **The State, Local, Tribal, and Territorial (SLTT) Grant Program:** This program has 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 current grant programs to provide cybersecurity assistance to SLTT entities has inherent flaws that this program will address. The program will be administered by FEMA in consultation with CISA acting as the subject matter expert.

- **DHS Science and Technology Directorate for Research and Development:** Allocates $31.5M per year over 5 years (total of $157.5M). 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:** This is a one-time investment of $35M in FY22 for Cybersecurity and Infrastructure Security Agency (CISA) to establish a capability to oversee and execute cross-sector governance to support CISA's national cross-sector coordination role, established in the FY21 NDAA.

- **Office of the National Cyber Director:** Allocates $21M in FY22 for a newly created office of The National Cyber Director (NCD). The NCD serves as a principal advisor to the President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders.