Plan for Assessing the Security and Resilience of Florida's Electric Grid and Natural Gas Facilities against Cyber and Physical Attacks

January 2025

TABLE OF CONTENTS

Figure **Page**

Tables **Page**

I. Executive Summary

The Legislature tasked the Florida Public Service Commission (Commission or FPSC), in consultation with the Division of Emergency Management and the Florida Digital Service, to develop and recommend a plan for conducting an assessment of "the security and resiliency of the state's electric grid and natural gas facilities against both physical and cyber threats." Ch. 2024-186, section 20, Laws of Florida.

If the Legislature decides to require an assessment be conducted, the Commission recommends that it primarily focus on the following five essential functions of a comprehensive cyber and physical security program:

- Risk Assessment and Mitigation
- Self-Evaluation of Processes and Internal Controls
- Regulatory Compliance
- Information and Operational Technology Protection
- Readiness Planning and Testing

Florida's electric and natural gas utilities recognize they must vigorously address each of these functions in their security programs and have dedicated substantial resources to maintain security and service reliability. Though specific regulatory requirements drive some activities, each utility exercises broad discretion in executing these functions. Utilities' risk profiles, financial resources, and subject matter expertise vary widely, as do the protection programs they deploy.

A. Scope

In developing a plan for assessing protections against cyber and physical attacks, the Commission recommends that the scope be focused upon these elements:

- The present and near-future challenges Florida's electric and natural gas utilities face within the constantly-evolving cyber and physical attack threat landscape. A description of the present threat landscape is provided in **Chapter II** of the report.

- The regulatory approach and compliance requirements presently in use by federal and state regulators to govern and assess the security and resilience of the electric and natural gas industries. **Chapter III** provides a description of the various governmental agencies involved in oversight of cyber and physical security protection, and their respective roles.

- The industry best practices regarding cyber and physical security currently being deployed by electric and natural gas utilities to maintain the security and resilience of critical assets and operations. The elemental functions and activities necessary for protection against attacks are discussed in **Chapter IV**.

- The challenge posed by the sensitive nature of utility cyber and physical protection efforts and the need for an assessment process to balance confidentiality concerns against statutory public disclosure requirements. These issues are discussed in **Chapter V** of the report.

B. Process Recommendations

In preparing an assessment plan, the Commission observes that the following initial steps would be advisable if the Legislature decides to require the assessment be implemented:

- Identify and define the appropriate role for Florida's state government to play in assessing the status of protections against cyber and physical attacks.

- Identify the duties, skillsets, and resources necessary to perform this defined role and assign responsibilities among state agencies or create a new organizational structure under the auspices of the State of Florida.

- Develop an assessment methodology that will overcome challenges posed by the highly sensitive nature of confidential utility information.

A collaborative approach to the assessment is recommended, seeking input and cooperation from utilities. Since the subject matter inherently involves a high degree of sensitivity and confidentiality, the assessment team would face challenges protecting the security of information. Fostering mutual trust and candor with Florida utilities would be essential. **Chapter V** of the report presents the Commission's analysis of these inherent confidentiality issues.

The Commission suggests a management audit methodology be used. The Commission's ongoing management audits, which began in 2013, have successfully monitored the status of the cyber and physical security protections of Florida's large electric utilities. Cooperation and extensive input from utilities will be vital to an assessment.

If a more hands-on, technical assessment is deemed necessary, the Legislature should assess the capabilities and skill sets available from state agencies. The use of outside subject matter expertise may be advisable.

C. Assessment Plan Recommendations

The Commission recommends an assessment plan should primarily focus on the following five essential functions necessary for maintaining comprehensive cyber and physical security programs:

- Risk Assessment, Monitoring, and Mitigation
- Self-Evaluation of Processes and Internal Controls
- Regulatory Compliance

- Information and Operational Technology System Protection
- Readiness Testing Activities

Within these five functions, the Commission recommends consideration of the following 16 descriptions of essential activities and approaches that are characteristic of effective utility cyber and physical security programs. Evaluation of the extent to which a utility has prioritized and undertaken these activities will provide the basis for assessing its preparedness against threats.

Risk Assessment, Monitoring, and Mitigation

Comprehensive approach to enterprise risk assessment and prioritization of responses

Ongoing monitoring of risks and development and execution of mitigation efforts

Self-Evaluation of Processes and Internal Controls

Risk-based program of internal audit activities to assess adequacy and effectiveness of internal controls and procedures

Ongoing self-evaluation of rigor and development of the cyber and physical security organization

Ongoing self-evaluation of voluntary adherence to National Institute of Standards and Technology (NIST) Cybersecurity Framework

Regulatory Compliance

Compliance with Federal Energy Regulatory Commission (FERC)-approved North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards and North American Energy Standards Board (NAESB) business practice standards

Compliance with applicable rules and regulatory requirements of Department of Homeland Security (DHS), Critical Infrastructure Security Agency (CISA), Transportation Security Administration (TSA), and Department of Energy (DOE)

Compliance with applicable state statutes, FPSC rules and orders, and participation in Commission's periodic operational reviews of cyber and physical security protections

Information and Operational Technology System Protection

Ongoing monitoring of critical systems access authorization for utility and third-party personnel, and through password and multi-factor authentication control procedures

Ongoing monitoring of server and application network environment configuration changes, system updates and patching, and maintaining records of Information Technology (IT) and Industrial Control Systems/Operational Technology (ICS/OT) system events and disruptions

Coordinated protections and separation of IT and ICS/OT systems

Rigorous supply chain screening and protection controls including upstream verification of vendor sourcing through software and hardware bill of materials, and damage protection contract language

Application of endpoint detection and response and threat-hunting tools (provided in-house or by consultants)

Readiness Testing Activities

Response and recovery planning, preparation, and updating of post-incident response and recovery plans

Testing attack readiness through facilities inspections and simulation exercises

Collaboration and information sharing through industry associations, law enforcement agencies, and Information and Sharing and Analysis Centers (ISACs)

D. Recommendations for Handling Sensitive Information

If the Legislature tasks an agency of the State of Florida to conduct or participate in an assessment of the security and resiliency of the state's electric grid and natural gas facilities, sensitive information could be exposed through the mandatory disclosure requirements of Florida's Public Records Law and the Government in the Sunshine Law. The Commission offers the following recommendations designed to protect such information handled by government agencies involved in the assessment and mitigate the risk of adverse impacts on the safe and reliable operation of the state's electric and natural gas infrastructure.

- Create statutory exemptions from disclosure requirements for the agency or agencies involved in conducting the assessment.
- Modify the statutory retention schedule and disposal process for information collected or transferred in the course of the assessment in order to maximize informational security.
- Establish a special commission or working group to conduct the security and resiliency assessment with explicit requirements to protect highly sensitive information.

II. Background and Perspective

A. Threat Landscape

The worldwide cyber and physical attack threat landscape for critical infrastructure involves various categories of malicious actors who deploy constantly-evolving attack vectors. Threat actors constantly develop methods of intrusion and refine existing ones. Targeted entities respond, attempting to detect, defeat, and ultimately prevent attacks of known types while attempting to catch up with new attack methods.

High-value targets within Florida's critical infrastructure sector include manufacturing, financial services, government, healthcare, and utilities. Several categories of malicious actors possessing differing levels of ability and sophistication maintain non-stop barrages of malicious probing. Collectively this activity takes the form of millions of daily intrusion attempts from varied techniques, such as simple phishing, unauthorized breach of IT and ICS/OT systems, data theft, malware insertion, and supply-chain infection.

In targeting electric and natural gas utilities, potential nation-state actors could seek out targets with the largest potential impact. By triggering cascading outages of portions of the national Bulk Electric Supply (BES) or disrupting the network of interstate natural gas transmission pipelines, actors could cripple parts of the U.S. for extended periods. Though generation reserve margins and intentional network layout redundancy provide a degree of protection, widespread extended electrical outages are more than theoretical possibilities. Specifically, BES interstate transmission lines and substations present the most impactful potential targets. As will be discussed in **Chapter III,** security and operation of these assets are largely subject to federal jurisdiction by agencies such as FERC, DOE, and DHS.

In response to the challenging threat landscape, Florida utilities are dedicating extensive resources to provide protection, detection, and recovery readiness. Ongoing risk assessments and security controls preparation and testing are conducted. Large utilities maintain a defense-in-depth strategy deploying sizeable staffs of cyber technology professionals, cooperating with relevant federal agencies to comply with rules and statutes. They are also scrutinizing supply chain vulnerabilities, making use of smart technology, and performing ongoing self-assessments.

1. Nation-State Threats

A growing number of known and suspected nation-state actor organizations pose the most serious threat to U.S. critical infrastructure. They wield substantial technical expertise and resource backing. The most active and sophisticated cyber attack organizations are sponsored by Russia, the Peoples Republic of China, the Islamic Republic of Iran, and the People's Democratic Republic of Korea.

Motivated politically, nation-state threat groups seek to disrupt operations, cause physical damage, steal intellectual property, and maintain long-term surveillance, often from within infiltrated IT systems. These activities present a serious national security risk that is managed by the Department of Defense (DOD), and federal intelligence agencies such as the Federal Bureau of Investigation (FBI).

2. Other Criminal Threats

Many cybercriminal threat actors deploy most of the same tactics as nation-state actors, but focus on generating financial gain through cyber attacks. This category of threat actors may have no political or social change motivation, but they may also provide services for hire to nation-states to assist in malware and ransomware attacks.

Ransomware has grown as an attack vector, leveraging system intrusions to yield payment of sizeable ransom demands. Following an intrusion, the threat actor succeeds in denying use of a system or application, while threatening to extract and release or destroy confidential information. As in human kidnapping cases, the intruder makes payment demands, provides instructions, and applies deadline pressure to rush the victimized entity to respond. A succession of threatened actions are presented to obtain compliance, though some may be calculated bluffs.

The FBI is the lead federal agency for investigating cyber attacks and intrusions. FBI investigations have led to the recovery of some ransom payments. However, once ransom demands are paid, it remains to be seen whether the attackers keep their promise to re-instate the denied system access or recover captured data. In some cases, where attackers kept promises to restore system use or return stolen data, they have issued statements that the intrusion was only executed for financial motives and not to cause damage or unrest.

B. Noteworthy Cyber and Physical Attacks

To date, despite the barrage of attempts and intrusions that have impacted various industry sector operations worldwide, no cyber or physical attack on the U.S. electrical grid has resulted in significant extended customer outages.

All attacks can provide lessons about the methods and capabilities of attackers. Several notable attacks within the U.S. and elsewhere are highlighted below as examples of various cyber and physical attack vectors, and the varying degrees of impact.

1. Russian Cyber Attacks on Ukraine

In 2015 and 2016, the "Sandworm" threat group, associated with the Russian government , triggered power outages in Ukraine using malware.[1] Attackers remotely switched off 30 substations by manipulating three Ukrainian distribution utilities' control systems. Power was interrupted for approximately three hours system-wide and about 230,000 customers lost power for up to six hours. In 2016, a fully-automated second cyber attack gained access to the Ukrainian utilities' networks. Sandworm used malware to attack a transmission system control center causing a portion of Kiev to lose power for an hour.

In April 2022, the Computer Emergency Response Team of Ukraine reported that Sandworm targeted a high-voltage electrical substation in Ukraine once again using malware. Sandworm planted the malware on systems within a regional Ukraine energy firm and moved laterally from

[1] Kim Zetter, "The Ukrainian Power Grid Was Hacked Again," *Vice Media*, January 10, 2017, https://www.vice.com/en/article/ukrainian-power-station-hacking-december-2016-report/.

the IT network. The attempt appeared to target the ICS/OT network with intent to send commands to substation devices controlling the flow of power. The cyber attack was detected and mitigated before a blackout occurred that could have potentially impacted up to two million people. This incident underscores the national security implications of cyber attacks.

2. SolarWinds Software Release

In December 2020, the most widespread supply chain malware attack to date in the U.S. was discovered. Malicious actors, directed by the Russian Foreign Intelligence Service, penetrated U.S. software developer SolarWinds, inserting malware into an update being developed for distribution to customers using SolarWinds' Orion business software.[2] The supply chain attack allowed hackers to access the network of U.S. cybersecurity firm FireEye, which provides hardware, software, and services to investigate cybersecurity attacks and protect against malicious software. FireEye detected the supply chain breach and recognized that attackers entered through a backdoor in the SolarWinds software via an update. 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 and Microsoft. SolarWinds stated that its customers included 425 of the U.S. Fortune 500 companies, the top ten U.S. telecommunications companies, electrical utilities, the top five U.S. accounting firms, all branches of the U.S. Military, the Pentagon, the State Department, and hundreds of universities and colleges worldwide. The malware was imbedded in the IT/OT systems of the impacted organizations and allowed the attackers to transfer and execute files, as well as profile and disable system services. Mitigation actions included rebuilding systems and improving threat detection and vulnerability testing. SolarWinds has since introduced new software development practices and technologies to strengthen its cybersecurity protections.

3. CrowdStrike Falcon Software Release

CrowdStrike is a software developer that offers Falcon, an endpoint detection and response software platform that uses artificial intelligence and machine learning to protect customer systems from the latest advanced threats. In February 2024, CrowdStrike developed and tested new software for Microsoft Windows and other systems that was integrated into the Falcon platform.

In July 2024, CrowdStrike released the software update, and an undetected error caused major disruptions to systems supporting aviation, banking, healthcare, and other industries. The effects of the incident were worldwide, impacting 8.5 million Windows devices and other IT systems. Remediation costs exceeded $700 million. Though this incident did not involve malicious actors like the SolarWinds "SUNBURST" supply chain attack, it illustrates the wide reach of a successful intentional attack.

---

[2]National Cyber Security Centre, "UK and US call out Russia for SolarWinds Compromise," April 15, 2021, https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

CrowdStrike has deployed process improvements and remediation steps, and its peer-reviewed analysis concludes that the incident is not exploitable in a way that achieves privilege escalation or remote code execution.

4. Colonial Pipeline Ransomware Attack

On May 7, 2021, Colonial Pipeline, a gasoline and jet fuel system serving the southeastern U.S., suffered a ransomware cyber attack. According to the FBI, the attack was the work of "REvil," a Russian-based hacking organization, and a closely-associated ransomware group known as "DarkSide."[3]

Colonial shut down its pipeline to contain the attack and prevent possible system damage. While the OT systems were not affected, the company's IT billing system was compromised. The six-day shutdown caused national impact and was the most successful cyber attack to date on a U.S. energy sector infrastructure target. Since a similar attack could also be executed against a large natural gas pipeline, the Colonial event heightened concerns about preparedness of natural gas pipeline companies.

Within several hours of the attack, Colonial paid the requested ransom of 75 bitcoins worth $4.4 million. The hackers did provide Colonial Pipeline the necessary software application to restore its network, but the network still operated very slowly. The restart of pipeline operations began at 5 p.m. on May 12, ending a six-day shutdown. On June 7, the Department of Justice (DOJ) announced that it had recovered 63.7 bitcoins worth $2.3 million of the company's payment, leaving Colonial with a loss of $2.1 million. Additionally, the Pipeline and Hazardous Materials Safety Administration (PHMSA) penalized Colonial $986,400 for control room management failures.

5. City of Oldsmar, Florida Water Plant ICS/OT Attack

In February 2021, the drinking water treatment facility for the City of Oldsmar, Florida was the target of a cyber attack. The municipally-owned facility provides water to businesses and 15,000 residents in Pinellas County, Florida. Unidentified cyber actors obtained access to the Supervisory Control and Data Acquisition (SCADA) system used for real-time monitoring of processes that control operational devices (e.g., pumps, switches, and valves). They accessed SCADA by exploiting cybersecurity weaknesses such as poor password security, an outdated operating system, and unprotected internet-based remote access software. This access enabled the cyber actors to increase the amount of caustic sodium hydroxide (lye) used in the water treatment process. Plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation. No customers or company personnel were harmed. Oldsmar's treatment process remained unaffected and continued to operate as normal, but the incident provided motivation nationwide for small water utilities to address the very basic protection weaknesses that were exploited.

[3]David E. Sanger and Nicole Pelroth, "F.B.I. Identifies Group Behind Pipeline Hack," *The New York Times*, May 10, 2021, https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html.

6. PIPEDREAM Malware Detected

"PIPEDREAM" is an ICS/OT malware attack framework with primary focus on critical infrastructure equipment and related technologies in oil, gas, and electric power operations. PIPEDREAM has been credited to a group named CHERNOVITE, which is believed to be a Russian state-sponsored threat actor.[4] According to the Critical Infrastructure Security Agency (CISA), advanced persistent threat actors have exhibited the capability to gain full system access to multiple ICS/SCADA devices. With access to ICS/SCADA devices, attackers could move laterally within the OT network to disrupt critical functions or devices.

After initial discovery in April 2022, a cybersecurity threat hunting consultant continued to observe and track PIPEDREAM to determine its capabilities and source. Natural gas and power generation industries may have been targeted. The discovery of PIPEDREAM is the first instance of pre-emptive detection of a major potential attack targeting ICS/OT. No damage or interruption of operations was caused, but the discovery of this threat has prompted widespread response by potential targets.

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

7. Physical Attacks on Substations

An April 2013 attack on Pacific Gas & Electric's Metcalf transmission substation near San Jose, California increased concerns about physical attacks on utility infrastructure. At least one shooter fired a rifle through a substation fence under cover of darkness resulting in more than $15 million in damage to 17 transmission transformers. PG&E was able to avoid any customer outages by rerouting its power supply. After the attack, FERC created CIP-014 imposing mandatory physical security standards for substations.

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

In 2022, a single shooter attacked an electric substation in North Dakota with a high-powered rifle causing $1.2 million in damage and power outages to 240 customers. The same shooter was eventually arrested after causing $495,000 of damage in 2023 to transformers at a pump station of the Keystone Pipeline in South Dakota. Though power outages in these attacks have not been significant, there is a substantial cost and supply chain lag time in replacing large substation transformers.

---

[4] Carolynn van Arsdale, "The Week in Security: Russian hackers targeted U.S. gas and electric, malicious PyPI packages show prowess," *Reversing Labs*, February 16, 2023. https://www.reversinglabs.com/blog/the-week-in-security-russian-hackers-almost-attacked-us-gas-and-electric-more-malicious-pypi-packages.

III. Current Oversight and Protections

A. Federal Jurisdiction

Several federal regulatory agencies have issued cyber and physical security standards and guidelines. Some of the standards are mandatory while others are voluntary. The responsibilities of these agencies overlap to an extent and continue to evolve. A simplified overview of the federal agency roles in cyber and physical security is presented in **Figure 1.**

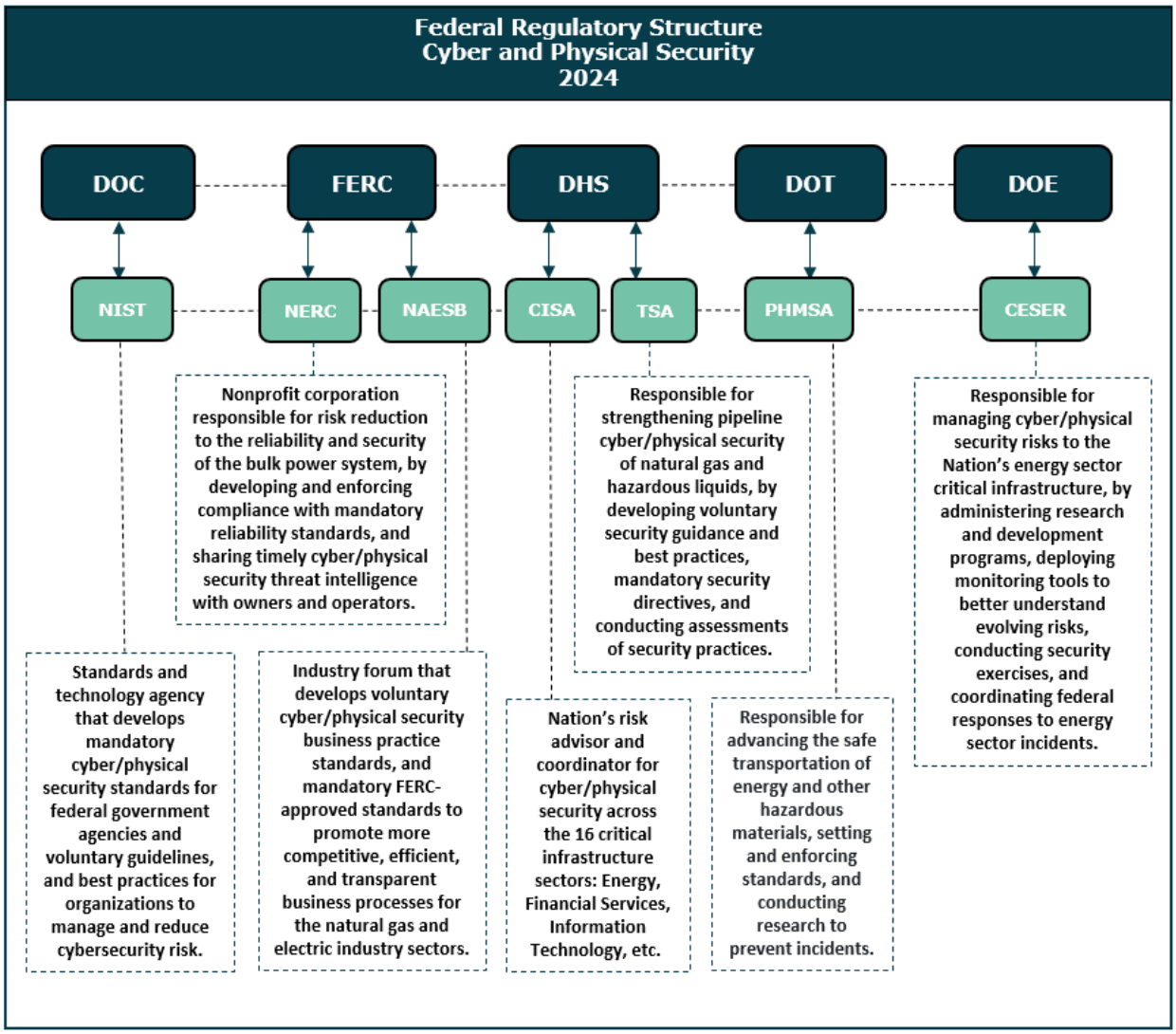

Figure 1

1. National Institute of Standards and Technology (NIST)

NIST, an agency within the Department of Commerce, is responsible for developing cyber and physical security standards, guidelines, best practices, and other resources for public and private-sector entities. The amended Federal Information Security Modernization Act of 2014 (FISMA) designated NIST as the lead federal agency to develop and promote technology standards and

guidelines. In response, NIST developed the framework for improving critical infrastructure cyber and physical security needed for FISMA compliance. The NIST Cybersecurity Framework is a set of voluntary best practices, standards, and recommendations to help owners and operators of critical infrastructure to manage and reduce their cyber and physical security risk and protect their networks and data.

Table 1 depicts the NIST Cybersecurity Framework's core functions and categories of activity. The framework outlines cybersecurity capabilities, projects, processes, and daily activities into six functions and 22 categories of activity. The six elemental functions (govern, identify, protect, detect, respond, and recover) provide a high-level view of an organization's functions and objectives for managing cybersecurity risk. Within these functions, the framework identifies 22 categories of activity essential to maintaining effective cybersecurity and physical security programs.

NIST Cybersecurity Framework 2024	
Function	**Categories**
Govern	*Organizational Context *Risk Management Strategy *Roles, Responsibilities, and Authorities *Policy *Oversight *Cybersecurity Supply Chain Risk Management
Identify	*Asset Management *Risk Assessment *Improvement
Protect	*Identity Management, Authentication, and Access Control *Awareness and Training *Data Security *Platform Security *Technology Infrastructure Resilience
Detect	*Continuous Monitoring *Adverse Event Analysis
Respond	*Incident Management *Incident Analysis *Incident Response, Reporting, and Communication *Incident Mitigation
Recover	*Incident Recovery Plan Execution *Incident Recovery Communication

Table 1

For most organizations, the NIST Cybersecurity Framework is best used as a starting point for implementing cyber and physical security programs and can guide an organization in determining the maturity level within each of the six functional areas.

2. Federal Energy Regulatory Commission (FERC)

The interstate transmission of electricity and natural gas is regulated by the FERC, an independent agency of the United States government. Unlike NIST's voluntary Framework, FERC's cyber and physical reliability standards are mandatory for the protection of the North American Bulk Electric System (BES). The BES, often referred to as "the grid," is the network

of interconnected electrical systems consisting of power generation, transmission facilities (rated at or above 100 kV) and control systems. The facilities and control systems are necessary to maintain an uninterrupted flow of electricity to homes and businesses across the country.

In 2003, the largest power outage in the history of North America was triggered by vegetation contacting overloaded transmission lines. Widespread blackouts were experienced by 50 million customers through the northeastern United States and Ontario. In response to this preventable event, Congress expanded FERC's role and jurisdiction pertaining to the BES, as discussed below.

a. North American Electric Reliability Corporation (NERC)

In 2006, FERC designated NERC as the Electric Reliability Organization (ERO) to develop and enforce mandatory reliability standards for the electric grid. In 2008, Critical Infrastructure Protection (CIP) reliability standards were introduced to safeguard the power grid from cyber and physical attacks. These standards required identifying and protecting critical assets, implementing security controls, and conducting regular assessments to ensure compliance. FERC may impose significant penalties for non-compliance. In 2014, NERC in partnership with NIST, mapped each CIP reliability requirement to the NIST Cybersecurity Framework function, category, and subcategory.

NERC CIP standards prescribe core protections and practices for designated assets owned and operated by electric utilities. NERC further oversees enforcement of CIP standards through a cyclical compliance audit program. Compliance failures may trigger sizable penalties, of as much as one million dollars per day per violation, and are resolved under additional scrutiny by NERC and FERC.

As directed by FERC, NERC develops revisions and additions to existing CIP standards that must be approved for enactment by FERC. **Table 2** lists the current 13 NERC CIP standards, which address requirements for identifying critical cyber assets, developing security management controls, training, facility security, supply chain risk management, use of firewalls, and incident reporting and recovery. Also shown is CIP-015, which is pending FERC approval. CIP-015 will require network security monitoring within trusted zones, such as electronic security perimeters, to effectively detect intrusions and malicious activity.

NERC Critical Infrastructure Protection Reliability Standards 2024		
Standard	**Title**	**Purpose**
CIP-002	BES Cyber System Categorization	Identify and categorize BES cyber systems and their associated BES cyber assets.
CIP-003	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	Personnel and Training	Require an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES cyber systems.
CIP-005	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	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	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	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	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	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	Information Protection	Prevent unauthorized access to BES cyber system information by specifying information protection requirements in support of protecting BES cyber systems against compromise.
CIP-012	Communications between Control Centers	Protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
CIP-013	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	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.
CIP-015 (Pending FERC Approval)	Internal Network Security Monitoring	Improve probability of detecting anomalous or unauthorized network activity to facilitate improved response and recovery from an attack.

Table 2

b. North American Energy Standards Board (NAESB)

NAESB is an industry forum for the development of standards to promote more competitive, efficient, and transparent business processes for the wholesale and retail natural gas and electric industries. NAESB standards development process involves support from DOE, FERC, NERC, NARUC, state utility commissions, and other governmental agencies at both the federal and state level. NAESB standards are adopted based on a consensus process and are initially voluntary; however, these become mandatory for public utilities upon approval by FERC. NAESB standards apply to four industry quadrants:

- Wholesale Gas Quadrant
- Retail Gas Quadrant
- Wholesale Electric Quadrant
- Retail Electric Quadrant

The standards within each quadrant continue to evolve to meet industry needs. For example, on September 19, 2024, FERC approved the most recent version of the business practice standards for the gas industry. The approved standards include revisions such as consolidating existing NAESB cybersecurity-related standards into a single manual. This effort should expedite the NAESB and FERC standards revision process. The standards strengthen cybersecurity protections through the use of secure communication and encryption methodologies, as well as measures to mitigate vulnerabilities such as:

- Using whitelisting and multi-factor authentication for file-to-file transactions.
- Incorporating firewalls, intrusion detection, and intrusion prevention system.
- Ensuring Open Access Same-Time Information Systems applications are secure against common industry recognized vulnerabilities.
- Applying software patches and updates in a timely fashion, ideally within seven days of availability.
- Performing quarterly vulnerability scans and penetration testing as well as annual business continuity and disaster recovery exercises.

3. Department of Homeland Security (DHS)

DHS is the federal executive agency responsible for public security. DHS has six overarching security plan initiatives, one of which is to secure cyberspace and critical infrastructure. The Homeland Security Act of 2002 gave DHS the overall responsibility to collaborate with government and private sector participants to develop the National Infrastructure Protection Plan (NIPP) to manage risk and achieve security and resilience outcomes. The initial version of the NIPP was released in 2006 and the most recent version in 2013 further integrates cyber and physical security planning.

The 2013 NIPP identifies 16 critical infrastructure sectors from all levels of government and industry, one of which is the energy sector. Other sectors, for example, include emergency

services, communications, food and agriculture. The NIPP directs DHS as the lead agency to coordinate with the critical infrastructure sectors to improve information sharing and collaboratively develop and implement risk-based approaches to cyber and physical security and the resilience of critical infrastructure assets, systems, and networks.

a. Cybersecurity and Infrastructure Security Agency (CISA)

In 2018, Congress passed the Cybersecurity and Infrastructure Act, establishing CISA within DHS. Its mission is to protect the nation's critical infrastructure from cyber and physical threats, and the networks of federal civilian agencies from cyber threats. CISA works with partners across government and industry to communicate current cyber trends and attacks, manage cyber risks, strengthen defenses, and implement preventative measures.

CISA develops and publishes rules for companies that provide critical infrastructure and will require reports of cybersecurity incidents within 72 hours and ransomware attacks within 24 hours. CISA provides alerts about current security issues, vulnerabilities, and exploits. CISA's Joint Cyber Defense Collaborative is a public-private partnership that proactively gathers, analyzes, and shares actionable cyber risk information to enhance cybersecurity planning, cyber defense, and response.

CISA further administers the Cyber Safety Review Board that conducts fact-finding and produces recommendations in the wake of major cyber incidents. The Board consists of cybersecurity experts from the private sector and senior officials from government agencies such as DHS, CISA, DOD, FBI, and Office of Management and Budget.

b. Transportation and Security Administration (TSA)

TSA is an arm of DHS charged with developing key policies and securing the nation's transportation systems (e.g., pipelines, ports, highways, railroads, and mass transit systems) from all threats, including physical and cyber attacks.

Prior to the Colonial Pipeline cyber attack in 2021, TSA's Pipeline Security Guidelines relied on voluntary industry compliance. Following the attack, TSA, in coordination with CISA, issued two Security Directives mandating that critical pipeline owners and operators implement cybersecurity measures. The first Directive required pipeline owners and operators of critical pipelines to designate a cybersecurity coordinator. The coordinator is required to be available to TSA at all times to coordinate cybersecurity practices and report any incidents to CISA. The report must identify any gaps, develop a remediation plan if necessary, and report the results to TSA and CISA.

The second Security Directive required owners and operators of critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to IT and ICS/OT systems. The Directive further required pipeline operators to implement a cybersecurity contingency and recovery plan, and to conduct a cybersecurity architecture design review.

In 2023, TSA updated its Security Directives to require oil and natural gas pipeline owners and operators to:

- Annually submit an updated cybersecurity assessment plan to TSA for review and approval.

- Annually report the results from the previous year's assessment, with a schedule for future assessment and auditing of specific cybersecurity measures for effectiveness. TSA requires all security measures of owners and operators to be assessed every three years.

- Develop and maintain a Cybersecurity Incident Response Plan (CIRP) that includes measures to be taken in the event of a cybersecurity incident.

- Test at least two CIRP objectives for effectiveness and include individuals serving in positions identified in the plan for their required annual exercises.

4. Department of Transportation (DOT)

While TSA's Security Directives require pipeline owners and operators to adequately prepare for and respond to cyber and physical attacks, the Pipeline and Hazardous Materials Safety Administration (PHMSA), within DOT, regulates the safe transportation of oil and gas pipelines. PHMSA oversees the safe design, operations, and maintenance of oil, gas, and other hazardous materials pipelines. This includes the oversight of pipeline control rooms and the ICS/OT side of pipeline operations.

PHMSA monitors compliance by operators of transmission and distribution pipeline systems through field inspections of facilities, operator management systems, procedures, and processes, and has a range of enforcement mechanisms and penalties for violations of its regulations. Although PHMSA does not have direct authority to regulate cyber and physical security, its safety oversight is clearly linked to security. PHMSA reviews and inspects the facilities and systems of owners and operators and enforces both safety and security-related requirements such as:

- Developing security plans that include elements such as personnel security, unauthorized access, and en-route security.

- Developing and maintaining emergency response information that includes mitigation measures to be taken when an incident occurs.

- Providing incident details to the National Response Center within one hour of discovery.

PHMSA and TSA have an interagency information-sharing agreement that enhances coordination efforts to advance pipeline safety and security, and improve information sharing on security incidents.

5. Department of Energy (DOE)

DHS designated the DOE as the lead agency to oversee energy sector security, which includes the electricity, oil, and natural gas industries. In partnership with DOE, the Electricity Sector Coordinating Council and the Oil and Natural Gas Coordinating Council developed an Energy Sector-Specific Plan (ESSP) to help achieve the following critical infrastructure security and resilience goals:

- Assessing security risks and threats
- Securing critical infrastructure from all hazards
- Enhancing critical infrastructure resilience
- Sharing information
- Promoting learning and adaptation

The approaches and activities discussed in the ESSP to support these goals are:

- Risk Management
- Interdependence and Coordination
- Information Sharing and Communication
- Critical Infrastructure Resilience and Preparedness

a. Risk Management

The energy sector faces a wide variety of risks that are evolving and may be difficult to assess or quantify due to a high level of uncertainty about the frequency or severity of events. Some of these risks include cyber and physical security threats. As such, the ESSP identified some initiatives undertaken by the energy sector to address these evolving risks.

One initiative is the DOE's development of the Energy Sector Cybersecurity Framework Implementation Guidance. The Guide is used to facilitate the energy sector's implementation of the NIST Cybersecurity Framework using existing sector-specific standards, tools, and processes to help the energy industry manage and protect its systems.

Another initiative is DOE's development, in collaboration with industry partners, of the Cybersecurity Capability Maturity Model (C2M2) to improve the energy sector's cybersecurity capabilities and to understand the cybersecurity posture of the industry. The C2M2 is a voluntary self-assessment used to evaluate, prioritize, and improve cybersecurity capabilities. C2M2 addresses new technologies such as cloud computing, mobile computing devices (e.g., smartphones and laptops), and artificial intelligence, as well as evolving threats such as ransomware and supply chain risks. It also included a secondary assessment to gauge a baseline maturity indicator level measurement for the ICS/OT environment. Two distinct C2M2s exist—one for the electric industry and another for the oil and natural gas industry.

b. Interdependence and Coordination

Technical innovations and developments in digital information and communications dramatically increased interdependencies among the nation's critical infrastructure sectors. Energy infrastructure provides essential fuel to all critical infrastructure sectors, and without energy, none of them can operate properly. Thus, its reliable operation is so critical that a disruption or loss of energy function will directly affect the security and resilience of other critical infrastructure sectors.

Both electricity and natural gas sector stakeholders in government and private sectors have undertaken a wide variety of approaches to address these concerns, including reliability assessments, interdependency studies, and coordinating activities, as well as policy reforms to

enhance the coordination and scheduling of natural gas pipeline capacity with electricity markets.

To better understand and mitigate potential impacts of cross-sector interdependencies, various regional and local exercises and coordinating activities are underway, including the Regional Resiliency Assessment Program. The program evaluates critical infrastructure from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, and resilience characteristics, as well as regional capabilities and gaps.

c. Information Sharing and Communication

The DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is the lead agency responsible for monitoring and responding to disruptions to the energy sector, including cyber and physical attacks. CESER works with state and local governments to share threat and intelligence information.

Many information sharing mechanisms exist between government and industry, within the critical infrastructure community, as well as through various industry trade associations. The Homeland Security Information Network (HSIN) provides a national platform to share homeland security information with sector partners. HSIN is a secure, web-based platform for sensitive, but unclassified information sharing and communication among federal, state, local, and private entities, as well as international partners. HSIN is just one of many information sharing mechanisms for critical infrastructure.

There are three key private sector information sharing tools in the energy sector: the Electricity Information Sharing and Analysis Center (E-ISAC), the Oil and Natural Gas ISAC (ONG-ISAC), and the Downstream Natural Gas ISAC (DNG-ISAC). These three ISACs serve the same objectives: collaboration, trusted information sharing, and timely threat intelligence analysis. Industry participation in the ISACs is voluntary.

d. Critical Infrastructure Resilience and Preparedness

Incident response planning and exercise is an essential part of the energy sector's resilience because preparation minimizes the disruption of critical infrastructure functions and associated consequences during an incident. Many incident response initiatives are in place to help maintain a secure, reliable, and resilient energy infrastructure. Preparation exercises are held at the federal, regional, state, local, and private levels, and are designed to prepare for and respond to incidents in order to minimize impacts resulting from a disaster. DOE and other government partners work with their industry partners for planning and encourage them to participate in the exercises.

To test these plans and response frameworks, government and industry participate in different exercises that may be organization-specific, regionally-focused, sector-specific, national, or international in nature. For example, NERC's biennial Grid Security Exercise (GridEx) allows participants to consider scenarios that impact their operations and require them to test response, mitigation, and recovery activities.

B. State Jurisdiction

Cyber and physical security protection efforts continue to rise to meet evolving threat vectors and methods trigger changes to federal protection standards and requirements. Florida utilities must continuously reassess protections and resource allocations. Cyber threats at the distribution energy resource level have increased significantly because of the increased interconnectivity of SCADA systems and public network infrastructure. As the penetration level increases, it is imperative to employ system-monitoring techniques and for state regulators to broaden their knowledge as they regulate public utility practices and cybersecurity.

Pursuant to Chapter 366, Florida Statutes (F.S.), the FPSC regulates all intrastate operational aspects, including rates and safety, of four investor-owned electric utilities and five investor-owned natural gas utilities. Chapter 366, F.S., also gives the FPSC jurisdiction over 35 municipal and 18 rural cooperative electric utilities with regard to rate structure, territorial boundaries, bulk power supply operations, and planning. Similarly, the FPSC has limited jurisdiction with regard to territorial boundaries for 27 municipal natural gas utilities and four gas districts. In addition, Chapter 368, F.S., gives the FPSC jurisdiction over the owners and operators of intrastate gas transmission and distribution facilities regarding their compliance with the FPSC's rules and regulations governing safety standards.

Relevant sections of Chapters 366 and 368, F.S., regarding jurisdiction over planning and development, safety standards, rates, and repair of facilities are provided in **Appendix 1**.

1. Electric Jurisdiction

FPSC jurisdiction is limited to electric distribution systems and local transmission facilities below a rating of 100 kV. However, NERC's national protection CIP reliability standards, under the authority of FERC, are designed to protect the BES, those transmission facilities rated at or above 100 kV. This jurisdictional separation is significant since the large transmission facilities under FERC jurisdiction are targets of far greater value and impact to large and sophisticated cyber attackers, particularly nation-state sponsored actors. The CIP standards impose a comprehensive set of requirements designed to protect critical cyber assets and ensure reliable operation of the BES.

Though distribution and lower voltage transmission lines under FPSC jurisdiction are interconnected with the BES, attacks on distribution facilities and low-voltage transmission facilities tend to produce localized outages that are easily resolved through switching activities. However, the continuing deployment of Distributed Energy Resources (DERs) also introduces potential cybersecurity challenges for electric utilities. DERs are small, modular energy generation and storage technologies, such as small wind turbines, rooftop solar systems, and battery storage. They are connected to the distribution system and often installed on the customer side of the meter.

Chapter 25-6, Florida Administrative Code (F.A.C.), is a set of agency rules that govern service provided by electric public utilities in Florida. The chapter is divided into several parts, including: records and reports, general management safety and reporting requirements, general service provisions, inspection of facilities, and notification of significant electrical outages and

events. **Appendix 2** highlights the rules of Chapter 25-6, F.A.C., relevant to protecting transmission and distribution facilities.

Florida's municipal electric utilities that are members of American Public Power Association are provided with a "playbook" to help them prepare a cyber incident response plan, prioritize their actions and engage predetermined contacts during cyber incident response, and coordinate messaging. The playbook serves three key purposes:

- Provides guidance to help develop a cyber incident response plan and outline the processes and procedures for detecting, investigating, eradicating, and recovering from a cyber incident.

- Maps out the industry and government partners that public power utilities can engage during a significant cyber incident to share information, get support for incident analysis and mitigation, and coordinate messaging for incidents that require communication with customers and the public.

- Outlines the process for requesting cyber mutual aid from utilities across the energy industry for a cyber event that significantly disrupts utility business or operational energy delivery systems and overwhelms in-house cyber resources and expertise.

Similarly, Florida electric cooperatives who are members of the National Electric Cooperative Association, have committed to use Essence, a market-ready early warning system that continuously assesses the electric grid for system anomalies. It was developed in collaboration with the DOE and is a cybersecurity tool used to protect key systems against unknown and emerging threats.

2. Natural Gas Jurisdiction

Natural gas is used by industrial, commercial, and residential customers, and fuels about 72% of Florida's electricity generation. It is transported to Florida customers through three major and two minor interstate pipelines regulated by FERC. The FPSC approves the need for certain new intrastate natural gas pipelines in Florida and is responsible for the safety of all natural gas operations within the state.

The American Gas Association is a primary source for natural gas utilities to stay abreast of federal government cyber and physical security initiative. For jurisdictional purposes, the FPSC is certified and authorized through PHMSA and Chapter 368, F.S., respectively, to physically inspect intrastate transmission and distribution pipelines. The FPSC has adopted the federal standards as well as more stringent regulations found in Chapter 25-12, F.A.C. PHMSA also authorizes the FPSC to conduct oversight and enforcement of pipeline operators through PHMSA's State Pipeline Safety Program. **Appendix 3** highlights some of the rules of Chapters 25-7 and 25-12, F.A.C., relevant to safety of gas transportation.

IV. Assessment Plan Recommendations

The Legislature tasked the FPSC, in consultation with the Division of Emergency Management and the Florida Digital Service, to develop and recommend a plan for conducting an assessment of "the security and resiliency of the state's electric grid and natural gas facilities against both physical and cyber threats." Ch. 2024-186, section 20, Laws of Fla. This Chapter sets forth the recommended areas of assessment. With any plan, the first step would be the framing of the scope of the assessment and the designation of a lead or coordinating organization under the auspices of the State of Florida to conduct the assessment. Options include state agencies, or the creation of a new entity to fulfill that role. Of particular concern will be the interaction of the assessment team with sensitive information, as discussed in **Chapter V**.

The assessment team can request each utility to describe and document how it addresses these key functions and activities, particularly how it evaluates their adequacy. This process would entail interviews of managers at many levels, and collection of documents such as risk assessments, recovery plans, internal audit reports, consultant reports, evidence of compliance with regulatory requirements, and readiness testing reports.

Within the five essential functions below, the Commission recommends evaluation of the utility's execution of the following activities and approaches characteristic of effective cyber and physical security programs. Evaluation of the extent to which a utility has prioritized and undertaken these activities will provide the basis for assessing its overall preparedness against attacks.

A. Risk Assessment, Monitoring, and Mitigation

Comprehensive approach to enterprise risk assessment and prioritization of responses

Utilities must take comprehensive ongoing efforts to stay abreast of both cyber and physical security risks. As in other areas of operations, the use of a risk register is necessary for identifying specific risks and tracking mitigation measures. Risk registers are also used in assessing the relative probability of negative risk outcomes, as well as their potential impacts.

Once the list of identified risks is compiled, ranking and prioritization of mitigation efforts can proceed. These decisions usually require direction and decision-making by senior managers within the organization. Regular review by senior management and the board of directors is appropriate. Due to the changing threat landscape, frequent review and revisions of the risk register are required.

Ongoing monitoring of risks and development and execution of mitigation efforts

Mitigation strategies, specific tasks, and timelines for each risk are identified in a risk register. The process of identifying and mitigating risks is a never-ending iterative process.

Mitigation tasks are broken down into subtasks, and assigned to units or individuals who can be held accountable. Ongoing feedback loops must be used to measure progress towards mitigating

each risk and to keep multiple levels of management up to date. Off-target results should trigger investigation and corrective action.

During this process, an ongoing probability versus magnitude of impact evaluation may be performed for each identified risk. This process assists the entity in prioritizing and targeting resources.

B. Self-Evaluation of Processes and Internal Controls

Risk-based program of internal audit activities to assess adequacy and effectiveness of internal controls and procedures

In all organizations, internal and external audits are the primary tool for assessing internal controls. A rigorous audit program is essential to determine the adequacy of cyber and physical security internal controls.

Audits are designed and prioritized on the basis of perceived risks for all areas of operations. These audits should address a variety of security-related issues such as patch management, insider risk management, network monitoring, and physical security management at selected facilities or locations. Changes in the threat environment or within internal processes require ongoing reassessment of the adequacy of internal controls and procedures.

The high degree of subject matter expertise required to evaluate cybersecurity protections may require use of external resources and consultants. This approach adds to the layering of defense in depth. Cybersecurity consultants specialize on areas, such as threat detection, penetration testing, and surveillance, that can greatly expand the scope of capabilities for even large utilities.

Maintaining compliance with the regulatory requirements mandated by various federal agencies requires constant vigilance. Some agencies perform periodic compliance audits, issuing findings that require management response and corrective action. Extensive efforts by utilities are required to track and implement required corrective action.

Ongoing self-evaluation of rigor and development of the cyber and physical security organization

As risks posed by potential cyber and physical security attacks grow, utility protection programs must increase in strength and maturity. To gauge this development, many utilities incorporate the DOE's C2M2 program as a foundational component of their cybersecurity risk management program. C2M2 is derived from multiple cybersecurity standards and frameworks, including NIST. The program assesses the maturity level of cybersecurity processes and practices. Each maturity rating level indicates a higher degree of protection capability.

Other models include Edison Electric Institute's "Culture of Security" self-assessment tool for utilities. A utility's internal or external audits may also provide evaluation of program maturity and overall capability.

Ongoing self-evaluation of voluntary adherence to the NIST Cybersecurity Framework
The NIST Cybersecurity Framework provides voluntary guidelines for developing an effective cybersecurity program. Most large utilities perform periodic reviews comparing their programs and processes to the recommendations of the NIST framework.

C. Regulatory Compliance

Compliance with FERC-approved NERC CIP reliability standards and North American Energy Standards Board (NAESB) business practice standards.
As discussed in **Chapter III**, FERC regulations, orders, and standards prescribe actions required of jurisdictional utilities. On behalf of FERC, NERC operates its Compliance Monitoring and Enforcement process, based on periodic audits of compliance with the CIP standards. Non-compliance can result in substantial fines and follow-up monitoring of corrective action. This process also relies on electric utilities self-reporting potential non-compliance issues. While self-reporting is voluntary, the practice is viewed favorably by the regulator and demonstrates a strong company culture of compliance.

FERC also approves NAESB business practice standards and communication protocols for natural gas and electric utilities. FERC conducts audits to ensure compliance with the NAESB standards and can impose penalties for non-compliance. The standards promote more competitive, efficient, and transparent business processes for the wholesale and retail natural gas and electric industries.

Compliance with applicable rules and regulatory requirements of DHS, CISA, TSA, and DOE
Several federal agencies play keys roles in the oversight of cybersecurity and physical security protections for electric utilities. They provide resources and collaboration to assist utilities in their efforts, and also issue standards and enforce compliance requirements.

These agencies include DHS, CISA, TSA, and the DOE. Within DHS, the TSA oversees directives and rules relating to the natural gas sector through its Pipeline Security Guidelines and Security Directives.

Compliance with applicable state statutes, FPSC rules and orders, and participation in Commission's periodic operational reviews of cyber and physical security protections
Investor-owned electric utilities and natural gas distribution utilities are subject to compliance with FPSC rules and statutory requirements.

Since 2013, the FPSC has performed periodic management audits regarding Florida's investor-owned electric utilities risk mitigation measures, internal controls, CIP compliance, employee training, attack simulation exercises, and recovery planning. Though this review process requires utilities to share sensitive information, care is taken to maintain confidentiality protections afforded by applicable statutes. Written reports summarize these reviews to update the Commission and staff regarding safeguards planned and in place.

D. Information and Operational Technology System Protection

Ongoing monitoring of critical systems access authorization for utility and third-party personnel, and through password and multi-factor authentication control procedures

Many cyber attacks begin with unauthorized system access through simple methods such as phishing or errors involving access card controls. Necessary access by contractors and other third-party personnel presents a challenge. Basic controls include password protection and multi-factor authentication control procedures, the effectiveness of which depends on employees' awareness and compliance.

Ongoing monitoring of server and application network environment configuration changes, system updates and patching, and maintaining records of IT and ICS/OT system events and disruptions

Basic necessary monitoring controls for utilities of all sizes include monitoring of server and application network environment configuration changes, system updates and patching, and maintaining records of IT and ICS/OT system events and disruptions.

Coordinated protections and separation of IT and ICS/OT systems

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

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

Rigorous supply chain screening and protection controls including upstream verification of vendor sourcing through software and hardware bill of materials, and damage protection contract language

Supply chain vulnerability continues to be a major concern and protection strategies have changed rapidly in response. To protect against supply chain compromise, utilities have updated supply chain standards to reflect current requirements, added protections into its contracts with third-party vendors, and continue to work with industry partners to execute upgrades and countermeasures as they become available. FERC has issued and updated CIP-013 standards in recent years. Many utilities have added damage protection contract language that indemnifies them against losses caused by vendors.

Although not explicitly mandated in the NERC CIP supply chain standards, utilities may request software and hardware vendors to provide a bill of materials. The utility's contract language may require vendors to apply industry best practice updates to antivirus and patching technology to manage the integrity of purchases to minimize security risk.

Application of endpoint detection and response and threat-hunting tools (provided in-house or by consultants)

By employing multiple layers of network monitoring, utility cyber defense teams detect and identify anomalous cybersecurity activity. Automated IT threat detection tools are available to detect, triage, and respond to attacks. Third-party consultants are employed to perform OT monitoring that provides threat detection and mitigation. Consultants may conduct penetration tests to identify weaknesses or vulnerabilities in systems, networks, human resources, or physical assets.

E. Readiness Testing Activities

Response and recovery planning, preparation, and updating of post-incident response and recovery plans

As part of the emerging cybersecurity threat, all Florida utilities prepare and periodically review recovery and business continuity plans. These activities have gone on for years. Vigilance to ongoing updates are necessary to reflect lessons learned from cyber and physical security incidents.

After a cyber or physical security incident, Florida utilities must be prepared to notify the appropriate contacts at the Florida Department of Law Enforcement Fusion Center, Florida Division of Emergency Management, and the Commission pursuant to Rule 25-6.018, F.A.C. Additionally, lines of communication should be prepared for necessary reporting to FERC, DHS, DOE and other agencies. For example, CISA, pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022, will require entities across all critical infrastructure sectors to report cyber incidents to CISA within 72 hours and any paid ransom demands within 24 hours.

Utilities must rely on automated tools and processes for backup and storage of information required to recover BES cyber system functionality. An ongoing secure system backup program is critical to recovery from malware and ransomware attacks.

Large and small utilities may benefit from participation in Edison Electric Institute's Cybersecurity Mutual Assistance Program. This assists smaller companies such as electric cooperatives and municipal utilities to leverage the resources of large utilities.

Testing attack readiness through facilities inspections and simulation exercises

Many utilities participate in or monitor NERC's biennial nation-wide GridEx security exercise or perform their own drills and exercises. Mock cyber drills and exercises enhance the ability to respond to cyber and physical security threats. Drills and programs range from malware detection, tabletop exercises, to activating command and control structures. Lessons-learned from testing should be used to update recovery plans.

Utilities also conduct periodic exercises to evaluate the adequacy of emergency response plans and preparedness that focus specifically on nuclear power plants. For example, the U.S. Nuclear Regulatory Commission (NRC) and Federal Emergency Management Agency (FEMA) created a

guidance document that requires nuclear power plant personnel to perform hostile action-based exercises during every eight-year planning cycle with federal, state, and local participation.

Collaboration and information sharing through industry associations, law enforcement agencies, and ISACs

Utilities share threat intelligence and risk mitigation measures through multiple government partners, vendors, industry groups, and regulatory entities to better manage and reduce security risks. The DHS's Cybersecurity and Infrastructure Security Agency provides alerts containing timely information about current security issues, vulnerabilities, and exploits.

DOE's Cybersecurity Risk Information Sharing Program (CRISP) is a public-private data sharing and analysis platform managed by NERC's Electricity Information Sharing and Analysis Center (E-ISAC) to facilitate sharing of cybersecurity threat information among energy sector stakeholders. Through partnership with energy sector owners and operators, CRISP leverages advanced sensors and threat analysis techniques developed by DOE to better inform the energy sector of high-level cyber risks. Participation in CRISP allows utilities to share real-time threat information anonymously and to identify additional safeguards as needed. CRISP also provides utilities access to FBI advanced threat intelligence.

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.

DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) in partnership with the National Association of Regulatory Utility Commissioners (NARUC) have established cybersecurity baselines for electric distribution systems and distributed energy resources. The partnership continues to develop implementation strategies and adoption guidelines with state regulatory agencies and industry stakeholders.

Local, state, and federal law enforcement agencies, such as local police, coast guard, and FBI, share potential security threat information. The FDLE oversees the Florida fusion centers. The exchange of information also exists through specific utility partnerships with InfraGard for seamless collaboration with the FBI Joint Terrorism Task Force and others including DHS and the Electricity Subsector Coordinating Council.

V. Analysis of Confidentiality Issues

A. Communicating, Collecting, Sharing, Storing, and Protecting Information

The Legislature tasked the Commission to develop and recommend a plan for conducting an assessment of "the security and resiliency of the state's electric grid and natural gas facilities against both physical and cyber threats." Ch. 2024-186, section 20, Laws of Fla. The Legislature specifically required the Commission to address "the manner in which information needed to conduct a security and resiliency assessment may be communicated, collected, shared, stored, and adequately protected from disclosure to avoid adverse impacts on the safe and reliable operation of the state's electric grid and natural gas facilities." *Id.* To address those issues as directed, this chapter will discuss:

- Information: What information is needed to assess physical and cyber security and resiliency;
- Protection: How security and resiliency information may be protected from statutory disclosure requirements; and
- Recommendations: Informational security considerations for a plan to assess physical and cyber security and resiliency.

1. Information: What Information is Needed to Assess Cyber and Physical Security and Resiliency

Conducting an assessment of the security and resiliency of the state's electric grid and natural gas facilities would require information such as:

- Technical Information: systems, infrastructure, architecture, capabilities, and weaknesses.
- Personnel Information: staffing levels, workgroup assignments, and security/resiliency employee depth chart.
- Operational Information: operational security plans, software update schedules, crisis management strategies.
- Incident Information: threat assessment strategies, crisis management plans, and restoration procedures.

This information would necessarily take the form of physical or digital records containing technical, logistical, and operational details related to physical and cyber security. As the Legislature has recognized, information of this nature could, if obtained by hostile actors, compromise the safety and reliability of Florida's critical energy infrastructure. *See* Ch. 2024-186, section 20. Therefore, paramount in a plan to conduct an assessment of security and resiliency is the protection of such records.

2. Protection: How Security and Resiliency Information May Be Protected From Disclosure requirements

In addition to the risk of disclosure due to physical and cyber threats, any agency or body of state or local government in Florida that conducts an assessment of the physical and cyber security and resiliency of the state's electric grid and natural gas facilities would be subject to the mandatory disclosure requirements of Florida's Public Records Law and the Government in the Sunshine Law, unless specifically exempted by the Legislature.

A. Public Records Law – Chapter 119, Florida Statutes

Florida's Public Records Law is contained in Chapter 119, F.S., which provides that any records made or received by any public agency in the course of its official business, as well as by any private entity acting on an agency's behalf, must be available for inspection by the public. *See* Section 119.07, F.S. The Commission is subject to the Public Records Law, as are all other agencies and governmental bodies created by law. Section 119.011(2), F.S.

The Public Records Law imposes on state agencies a broad requirement to disclose public records upon request by any member of the public. A public record is defined as "all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency." Section 119.011(12), F.S. The Florida Supreme Court has interpreted this definition broadly to encompass all "material(s) prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type." *Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc.*, 379 So. 2d 633, 640 (Fla. 1980). Public records must be maintained and stored according to the requirements of Section 119.021, F.S. All public records must be kept in the buildings in which they are usually used, a custodian of public records at that agency must keep such records safe and accessible for use, the records must be restored if they are damaged, and the agency must comply with retention schedules and disposal processes established by the Division of Library and Information Services of the Department of State. *See* Section 119.021, F.S.

The only exceptions to the disclosure requirements of the Public Records Law are those specifically created by statute. *See, e.g.*, *Wait v. Florida Power & Light Co.*, 372 So. 2d 420, 425 (Fla. 1979) (The Public Records Act "excludes any judicially created privilege of confidentiality and exempts from public disclosure only those public records that are provided by statutory law to be confidential or which are expressly exempted by general or specific law."); *Times Pub. Co., Inc. v. City of St. Petersburg*, 558 So. 2d 487, 492 (Fla. 2d DCA 1990) ("In fact, the right to access public documents is virtually unfettered, save only the statutory exemptions designed to achieve a balance between an informed public and the ability of the government to maintain secrecy in the public interest.")

In light of the broad scope and liberal construction of the Public Records Law, information needed to assess the security and resiliency of Florida's electric grid and natural gas facilities would ordinarily be subject to disclosure, unless the Legislature provides an express statutory exemption in order to avoid adverse impacts on the safe and reliable operation of critical energy infrastructure.

For example, Section 119.0725, F.S., exempts records related to cybersecurity and critical infrastructure from the disclosure requirements of the Public Records Law. The exempt information includes cybersecurity incident information reported pursuant to state law. Section 119.0725(2)(c), F.S. *See also* Section 282.318, F.S. (protecting state agency data, information, and technology that is gathered pursuant to risk assessments and other reports made by state agencies under the statute). Additionally, Section 119.0725, F.S., exempts from disclosure information relating to "critical infrastructure," which is defined as "existing and proposed information technology and operational technology systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health, or public safety." Section 119.0725(1)(b), F.S. However, this exemption may only protect records related to the *agency's* cybersecurity and critical infrastructure, and this may not be applicable to the information required for an agency to perform an assessment of the security and resiliency of utility-owned facilities and infrastructure in Florida.

Additionally, Section 119.0713(5)(a), F.S., is an exemption that applies to information held by a utility owned or operated by a unit of local government. In particular, the statute exempts from disclosure information related to the "security of the technology, processes, or practices . . . designed to protect the utility's networks, computers, programs, and data from attack, damage, or unauthorized access, which information, if disclosed, would facilitate the alteration, disclosure, or destruction of such data or information technology resources." Section 119.0713(5)(a)1., F.S. This exemption also protects "[i]nformation related to the security of existing or proposed information technology systems or industrial control technology systems" where its disclosure "would adversely impact the safe and reliable operation of the systems and the utility." Section 119.0713(5)(a)2., F.S. However, because this exemption applies only to information held by a municipally owned utility, it would likely not apply once the information passed into the possession of a third party, such as a government agency conducting an assessment of the security and resiliency of the utility's cybersecurity and critical infrastructure.

There are also existing exemptions related to certain information received by the Commission from public utilities providing electricity or gas to the public when disclosure could be detrimental to the business interests of the utility providing the information. Specifically, Section 366.093, Florida Statutes, exempts from public disclosure "proprietary confidential business information," which the statute defines as:

> [I]nformation, regardless of form or characteristics, which is owned or controlled by the person or company, is intended to be and is treated by the person or company as private in that the disclosure of the information would cause harm to the ratepayers or the person's or company's business operations, and has not been disclosed unless disclosed pursuant to a statutory provision, an order of a court or administrative body, or private agreement that provides that the information will not be released to the public.

Section 366.093(1), (3), F.S. There is an identical exemption relating to information received by the Commission from natural gas transmission companies. *See* Section 368.108, F.S. However,

the statutes provide that the Commission shall apply the exemption only "upon request of the public utility or other person" and when "shown and found by the Commission to be proprietary confidential business information." *See, e.g.*, Section 366.093(1), F.S.

While some of the exemptions discussed above may apply to the kind of information required to conduct a security and resilience assessment of Florida's electricity grid and natural gas facilities, Florida courts tend to construe exemptions narrowly in furtherance of the legislative policy favoring disclosure. *See, e.g.*, *Rameses, Inc. v. Demings*, 29 So. 3d 418, 421 (Fla. 5th DCA 2010) (stating that "[i]n light of the policy favoring disclosure, the Public Records Act is construed liberally in favor of openness, and exemptions from disclosure are construed narrowly and limited to their designated purpose"). Therefore, proceeding with such an assessment without an explicit statutory exemption that specifically protects sensitive information related to security and resiliency risks could result in adverse impacts to Florida's electric grid and natural gas infrastructure due to the broad disclosure requirements of Florida's Public Records Law.

B. Sunshine Law – Chapter 286, Florida Statutes

Another manner in which sensitive information related to the security and resiliency of Florida's electricity and natural gas infrastructure could be exposed is through the meetings and discussions of the agency conducting the assessment. Florida's Government in the Sunshine Law ("the Sunshine Law") is found in Section 286.011, F.S., and requires that all meetings of any board or commission of any state or local agency be open and accessible to the public. It provides that "all meetings . . . at which official acts are to be taken are declared to be public meetings open to the public at all times, and no resolution, rule, or formal action shall be considered binding except as taken or made at such meeting." *Id.* Additionally, all such meetings must be noticed and publicly available, and information communicated by government officials must be stored and available to members of the public upon request. *Id*.

The Sunshine Law would likely require any meeting at which official action is taken by a commission or board conducting an assessment of the security and resiliency of Florida's electric grid and natural gas facilities to be open and accessible to the public, which could compromise confidentiality of sensitive security information. The Commission has a statutory exemption for hearings at which certain confidential or sensitive matters are discussed. *See, e.g.*, Section 350.01(9), F.S. If the Legislature desires to protect such information from disclosure, the commissions or boards participating in the assessment should similarly be exempted from the requirements of the Sunshine Law with respect to the meetings discussing this type of information.

3. Recommendations for Handling Sensitive Information

In Chapter 2024-186, section 20, the Legislature requires the Commission to include in this plan certain recommendations addressing how information related to cyber and physical security of the electric grid and natural gas facilities may be protected from disclosure in order to avoid adverse impacts to safe and reliable operation. If the Legislature decides that an agency of the State of Florida shall conduct the assessment, the Commission's recommendations are below:

A. Create Statutory Exemptions From Disclosure Requirements

As discussed above, existing exemptions from the statutory disclosure requirements of the Public Records Law and the Sunshine Law may not be sufficient to protect the sensitive information received from public utilities and other private entities in connection with a security and resilience assessment. Therefore, legislation may be required to ensure that such information is protected from disclosure by specific and explicit statutory exemptions.

Thus, we recommend that the Legislature consider the creation of a distinct and explicit exemption from the disclosure requirements of the Public Records Law and the Sunshine Law. This would ensure that, regardless of which agency or agencies are tasked with conducting or participating in the assessment, sufficient statutory protection is in place to maintain the confidentiality of sensitive security information. We recommend that the Legislature consider including the following elements in such an exemption:

- A rebuttable presumption of confidentiality for records received and meetings conducted in the course of the assessment that relate to cyber and physical security and resilience of the electricity grid and natural gas facilities.

- A minimum term of confidentiality, after which time the utility or entity that provided the information may petition to either continue the confidential status or return the information.

- A requirement that the agency or agencies conducting the assessment return or destroy all confidential information upon final completion of the assessment process.

An exemption that includes the elements above, as well as any other such provisions the Legislature deems appropriate or necessary, would sufficiently protect the information needed to conduct a security and resiliency assessment in order to avoid adverse impacts on the safe and reliable operation of the state's electric grid and natural gas facilities.

B. Transmission of Information to Other Governmental Entities

Due to the cooperation required among public and private entities to conduct a security and resiliency assessment of Florida's energy infrastructure, there is a concern that such cooperation could unintentionally increase the risk of disclosure. Unnecessarily multiplying the number of individuals in possession of confidential records or increasing the number of "custodian[s] of public records" for purposes of the Public Records Law could enhance the risk that such information will be discovered or disclosed. *See* Sections 119.011(5), 119.07, F.S. Additionally, the number of public employees in possession of sensitive material could be increased by the provision of the Public Records Law that requires agencies to adhere to the public record retention schedules and disposal process established by the Division of Library and Information Services of the Department of State. *See* Section 119.021, F.S. If each employee is required to retain a copy of the public record, then a longer retention schedule could result in more employees in possession of the same record. Due to the highly sensitive nature of the information

at issue, we recommend that the Legislature mitigate this increased risk of disclosure in some way.

For example, the Legislature could exempt the information related to the security and resiliency assessment from the ordinary retention schedule and disposal process. The Legislature could either establish a special retention schedule and disposal process for the information related to the assessment and or allow the agency conducting the assessment to establish its own schedule. We recommend that the retention schedule and disposal process require disposal of records a certain number of days after transfer in order to limit the number of public employees in possession of sensitive information. In any case, the retention and disposal requirements applicable to the agency and information related to an assessment of the security and resiliency of the electric grid and natural gas facilities in Florida should be particularized to provide maximum informational security.

C. Establish a Special Commission or Working Group to Conduct the Security and Resiliency Assessment

Given the unique and highly sensitive nature of the information needed to conduct an assessment of the security and resilience of the state's electric grid and natural gas facilities, and in light of the adverse consequences of potential disclosure of such information, the Legislature should consider designating a lead or coordinating organization under the auspices of the State of Florida to conduct the assessment. This would allow the Legislature to craft unique requirements and exemptions that could adequately protect from disclosure the information that, in hostile hands, could compromise the safe and reliable operation of vital energy infrastructure. As the agency charged with economic regulation of public utilities, we recommend that at least one representative from the Commission participate in any assessment plan process to provide subject-matter expertise.

B. Conclusion

The Legislature has established a state policy that all state records be kept open for personal inspection and copying by any person. *See* Section 119.01(1), F.S. The Legislature also recognizes that the disclosure of information needed to conduct a security and resiliency assessment could result in adverse impacts on the safe and reliable operation of the state's electric grid and natural gas facilities. *See* Chapter 2024-186, section 20. Therefore, such an assessment must balance the two policy goals in the interest of public safety. We recommend that the Legislature ensure that any organization tasked with conducting the assessment be given clear directives and protections that will enable it to maintain the safety, reliability, and security of the state's energy infrastructure while safeguarding the public trust.

VI. Appendices

A. Appendix 1

FPSC Electric and Gas Jurisdiction Chapters 366 and 368, F.S. 2024	
Section	**Purpose/Description**
366.04(5)	Grants the FPSC "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."
366.04(6)	Gives the FPSC "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…"
366.05(1)(a)	Requires the FPSC "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 FPSC can also require "repairs, improvements, additions, replacements, and extensions to the plant and equipment of any public utility when reasonably necessary…"
366.05(8)	The FPSC 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…"
368.05(1)	Grants the FPSC "jurisdiction over all persons, corporations, partnerships, associations, public agencies, municipalities, or other legal entities engaged in the operation of gas transmission or distribution facilities with respect to their compliance with the rules and regulations governing safety standards..."
368.05(2)	The FPSC may require Florida gas utilities to file "periodic reports and all other data reasonably necessary to determine whether safety standards prescribed by it are being complied with; may require repairs and improvements to the gas transmission and distribution piping systems…"
368.104	Requires the FPSC "to fix and regulate rates and services of natural gas transmission companies, including, without limitation, rules and regulations for determining the classification of customers and services, for determining the applicability of rates, and for ensuring that the provision (including access to transmission) or abandonment of service by a natural gas transmission company is not unreasonably preferential, prejudicial, or unduly discriminatory…"

B. Appendix 2

FPSC Electric Jurisdiction Chapter 25-6, F.A.C. 2024	
Rule	**Purpose/Description**
25-6.018	**Records of Interruptions and Commission Notification of Threats to Bulk Power Supply Integrity or Major Interruption of Service**, … notification of certain situations, including any bulk power supply malfunction or accident which constitutes an unusual threat to the bulk power supply integrity.
25-6.0183	**Electric Utility Procedures for Generating Capacity Shortage Emergencies**, adopts the Florida Reliability Coordinating Council's Generating Capacity Shortage Plan … to address generating shortage emergencies within Florida.
25-6.0185	**Electric Utility Procedures for Long-Term Energy Emergencies**, … requires a long-term energy emergency plan to establish a systematic and effective means of anticipating, assessing, and responding to a long-term emergency caused by a fuel supply shortage.
25-6.019	**Notification of Events**, … must report to the Commission within 30 days of learning about any event involving a portion of the electrical system involving damage to the property of others in excess of $10,000, or causing significant damage in the 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 by reference the 2017 National Electrical Safety Code (NESC) C2-2017, as the applicable safety standards for transmission and distribution facilities subject to the Commission's safety jurisdiction. Each investor-owned electric utility, rural electric cooperative, and municipal electric system shall, at a minimum, comply with the standards in these provisions.
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.

C. Appendix 3

FPSC Gas Jurisdiction Chapters 25-7 and 25-12, F.A.C. 2024	
Rule	**Purpose/Description**
25-7.018	***Record of Interruptions,*** … requires each utility to keep a complete record of all interruptions affecting the lesser of 10 percent or 500 or more meters including cause, date, time, duration, remedy, and steps taken to prevent recurrence, … and to notify the FPSC as soon as detected and provide a report after service restoration.
25-12.005	***Codes and Standards Adopted,*** … requires operators of natural gas pipeline facilities to comply with the PHMSA standards in 49 C.F.R. Parts 191 and 192. …
25-12.007	***Commission Compliance Evaluations,*** … requires FPSC or its authorized representatives to be granted access to all installations or construction projects, … to records or data related to compliance with these rules, standards, or codes.
25-12.009	***Safety,*** … requires each operator to establish a continuing education program to enable customers and public to recognize a gas pipeline emergency for the purpose of reporting it to the operator, … and reduce hazards to employees, customers, and the public, …
25-12.020	***Construction Specifications and Inspections,*** … requires each operator to formulate comprehensive written construction specifications for all phases of design, installation, testing, repair, and inspection … to assure compliance with these rules, … to conduct field inspections, … and to have qualified inspectors to detect and correct any component that fails to meet these rules or construction specifications.
25-12.022	***Requirements for Distribution System Valves,*** … requires installing valves upstream of each regulator station for use in an emergency to stop the flow of gas, … sectionalizing valves, … identifying emergency or sectionalizing, and other critical valves designated on appropriate records, drawings, or maps used by the operator and referenced to above-ground structures so readily located, … protecting blowdown valves against tampering and mechanical damage,… and inspecting all valves necessary for safe system operation.
25-12.041	***Receiving of Gas Leak and Emergency Reports,*** … requires each operator to have an operating/maintenance plan containing procedures for receiving and promptly responding to reported gas leaks and emergencies on a 24-hour per day basis. …
25-12.042	***Investigation of Gas Leak Reports,*** … requires each operator to consider gas leaks reported by customers or the general public as emergencies requiring prompt response with the first priority of protecting life then property, …
25-12.044	***Interruption of Gas Service,*** … requires each operator, at the time gas service is turned off or when aware gas to a customer has been interrupted, to either lock the valve of the service line in the closed position or … plug it to prevent the flow of gas.
25-12.060	***General Records,*** … requires each operator to retain all tabulations, standards, drawings, or other records of incidents, procedures, or studies related to the compliance with these rules and adopted standards and codes, …
25-12.062	***Leak Reports,*** … requires records of gas leaks on the operator's system to show as a minimum: address of suspected leak, date/time reported, description of leak reported, date/time dispatched, worked, resolved, and leak location, and cause.
25-12.084	***Notice of Accidents and Outages,*** … requires each operator at the earliest time after detection of an incident involving the release of gas from a pipeline to give telephonic notice to the FPSC, … and to include impact and all other data required by this rule, … and to immediately report to the FPSC any incident that interrupts service to either 10 percent or more of its meters or 500 or more meters.

D. Appendix 4

Glossary of Terms

Attack Vector	A method used to gain unauthorized access to a system, network, or application. Attack vectors can be technical or human-based, and can target many different components of an organization's infrastructure.
Bulk Electric System (BES)	All Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.
Critical Infrastructure	The systems and assets that are vital to the functioning of society, and whose destruction or exploitation could have serious consequences, including customer outages.
Critical Infrastructure Protection (CIP) Reliability Standards	A set of mandatory FERC cyber and physical security regulations and guidelines designed to protect the BES from cyber threats.
Cyber Attacks	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
Cybersecurity Capability Maturity Model (C2M2)	A model approved by DOE available to utilities to assess protection of critical assets and infrastructure. C2M2 is used to evaluate cyber risks, measure cybersecurity program maturity, strengthen operational resilience, optimize security investments, and achieve regulatory compliance.
Federal Energy Regulatory Commission (FERC)	The federal agency with primary jurisdiction over the interstate transmission of electricity, natural gas, and oil. FERC enforces mandatory cyber and physical security reliability standards for the protection of the BES.
Industrial Control Systems (ICS)	Utility devices, controls, and processes that provide remote automated operation and electronic reporting. ICS include systems such as Supervisory Control and Data Acquisition (SCADA).
Operational Technology (OT)	OT is a broad range of hardware and software that detects or causes a change through the direct monitoring and control of devices, processes, and events in the physical environment. Examples include physical access control systems, and transportation systems.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Intrusions	A security event, or a combination of multiple security events, in which an intruder gains, or attempts to gain, unauthorized access to a system or system resource. Some intrusions may not be detected, leading to further undetected manipulation of systems, data capture, or denial of use.
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
Multi-Factor Authentication	An authentication method that requires the user to provide two or more verification steps to gain access to a resource such as an application or an online account.
National Institute of Standards and Technology (NIST) Cybersecurity Framework	A voluntary set of standards and best practices available to utilities to better manage and reduce cybersecurity risks. The Framework provides a structured approach to assessing, monitoring, and remediating existing and potential threats.
Physical Attacks	A direct action targeting a utility's tangible assets, such as IT systems, equipment, or infrastructure. Physical attacks can result in unauthorized access to sensitive data, hardware, or software.
Ransomware	A malicious attack where attackers seize control of and encrypt a utility's data and demand payment to restore access.
Supervisory Control and Data Acquisition (SCADA)	A computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems.
Threat Group	A collection of individuals or a coordinated organization with malicious intent, working to carry out cyber attacks, exploiting vulnerabilities, seizing data, or disrupting operations.
Whitelisting	A list of entities that are authorized to be active or present on systems. Whitelisting identifies and blocks potential intruders, preventing infiltration of malware, unlicensed software, and other unauthorized software.