



Writer's Direct Dial Number: (850) 521-1706
Writer's E-Mail Address: bkeating@gunster.com

August 22, 2024

BY E-FILING

Mr. Adam Teitzman, Clerk
Florida Public Service Commission
2540 Shumard Oak Boulevard
Tallahassee, FL 32399-0850

Re: Docket No. 20240099-EI - Petition for rate increase by Florida Public Utilities Company


Dear Mr. Teitzman:

Attached, for electronic filing, on behalf of Florida Public Utilities Company, please find the Testimony and Exhibits of Vikrant Gadgil.

Thank you for your assistance with this filing. As always, please don't hesitate to let me know if you have any questions whatsoever.

(Document 8 of 18)

Sincerely,



Beth Keating
Gunster, Yoakley & Stewart, P.A.
215 South Monroe St., Suite 601
Tallahassee, FL 32301
(850) 521-1706

1 BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

2 Docket No. 20240099-EI: Petition for rate increase by Florida Public Utilities Company,
3 Electric Division

4 Prepared Direct Testimony of Vikrant Gadgil

5 Filed: August 22, 2024

6 **Q. Please state your name, occupation and business address.**

7 A. My name is Vikrant A. Gadgil and my business address is 500 Energy Lane, Dover
8 Delaware 19901.

9 **Q. By whom are you employed and in what capacity?**

10 A. I have been employed by Chesapeake Utilities Corporation as the Senior Vice
11 President and Chief Information Officer (“CIO”) since 2015. In this capacity, I am
12 responsible for leading the Information Technology (“IT”) team, as well as the
13 development and implementation of the strategy for supporting and enhancing our
14 technology platforms, including data networks and cybersecurity, telephony,
15 computing infrastructure, business systems and applications, for all businesses under
16 the Chesapeake umbrella, including Florida Public Utilities Company.

17 **Q. Describe the scope of your responsibilities.**

18 A. The IT function team is staffed by approximately 40 employees and is responsible
19 for the holistic, complete support of 1300+ employees, multiple contractors, and all
20 functions and business units at Chesapeake Utilities Corporation across multiple
21 physical sites. The key responsibilities of the IT function include ensuring a reliable,
22 available, and secure communication network, maintaining customer data security,
23 enabling data analytics tools and services, and supporting business applications

1 across all corporate functions including, but not limited to, billing, financial systems,
2 work order management, human resource information systems, geographic
3 information systems, Outage Management, email, and office productivity tools.

4 **Q. Please describe your educational background and professional experience.**

5 A. Prior to joining Chesapeake Utilities Corporation, I held the position of Deputy CIO
6 and was the Senior Director for Global Project Management Office and Information
7 Security at Vishay Intertechnology, Inc., a Fortune 1000 company. Prior to joining
8 Vishay Intertechnology, Inc., I held various leadership positions in IT with Procter &
9 Gamble and Ecolab, Inc., which are leading global companies.

10 I have over 30 years of experience in the IT industry. I hold a Bachelor of
11 Engineering degree in Electrical Engineering from the National Institute of
12 Technology, India and an MBA from the Indian Institute of Management – Calcutta
13 India.

14 **Q. How will you refer to the Company?**

15 A. When referring to the Florida Public Utilities Company Electric Division, I will refer
16 to it as “FPUC” or “the Company”. When referring to Chesapeake Utilities
17 Corporation, the parent company, I will refer to it as “CUC” or the “Corporation.”

18 **Q. Have you filed testimony before the Florida Public Service Commission in prior
19 cases?**

20 A. Yes, I have filed testimony in Docket No. 20220067-GU.

21 **Q. Have you previously provided testimony before other regulatory bodies?**

22 A. No, I have not.

23 **Q. What is the purpose of your testimony in this proceeding?**

1 A. My testimony will discuss the following topics:

2 (i) Technology advancements implemented since the Company's last rate case;

3 (ii) Planned new technology implementation; and

4 (iii) Improvements in cyber security.

5 **Q. Are you sponsoring any MFRs in this case?**

6 A. Yes. I have attached as Exhibit VG-1 is a list of Minimum Filing Requirements that I
7 co-sponsored.

8

9 **IT SERVICE LEVELS**

10 **Q. Please provide an overview of the changes in IT that the Corporation has**
11 **implemented in recent years to the benefit of the Company's customers.**

12 A. Consistent with the ever-evolving technological landscape and changing needs of our
13 businesses, the Company has strengthened its IT software, computer and
14 telecommunications hardware, and network infrastructures to include necessary
15 additional functionalities, as well as to ensure key financial, billing and other
16 systems can be maintained in a safe manner without interruption even as we increase
17 our use and reliance upon these key systems. IT has also increased its staffing, as
18 well as the expertise of its staff, to address increased external risks, largely
19 associated with cyberattacks, and to meet increasing demands for service.

20 Since its acquisition in October 2009, FPUC has benefited significantly from CUC's
21 enhanced IT infrastructure as it has enabled FPUC to provide better customer service
22 through: (1) its enhanced website; (2) more secure customer billing and enhanced
23 protections for customer personal information; (3) deployment of technology to

1 enable employees to work remotely, which, among other things, provided necessary
2 flexibility and resilience in operations during the COVID-19 pandemic; and (4)
3 implementation of a compliance management system by using IFS AB, a leading
4 enterprise software company and leading provider of enterprise resource planning
5 solutions. In addition, CUC's technology enhancements have ensured that FPUC has
6 the most accurate and timely financial information available as necessary for
7 strategic planning and critical business decisions.

8 The technology landscape continues to evolve at a rapid pace in order to keep up
9 with continually changing customer, employee, and stakeholder expectations. The
10 availability, reliability and performance of our technology infrastructure is key to the
11 regular operations of all of CUC's business units, but also is key to our ability to
12 address emergency events, as well.

13

14 **TECHNOLOGY ADVANCEMENTS**

15 **Q. What are some of the areas in which the Corporation has deployed newer,**
16 **advanced technologies and applications?**

17 A. Digital transformation is critical to the core operations of all CUC's business units.
18 CUC is constantly investigating new ways to incorporate the power of data and
19 communications technology to improve services and increase efficiency for our
20 customers. Since 2013, the key technology developments impacting CUC and its
21 businesses have involved the expansion of mobile computing, the emergence of
22 smartphones, network upgrades, enhanced social media and an expanded number of
23 platforms, predictive analytics, and hyper-converged infrastructure. In addition, our

1 bandwidth requirements on wireless and wide area networks have increased to keep
2 up with the upgrades in our capabilities and tools.

3 Cyber security is critically important for data and information security as well as
4 operational reliability. Threat actors include, among others, nation states, organized
5 criminals driven by profit motive, as well as opportunistic attackers. The goals of
6 the threat actors can include extortion through threat of data infiltration or
7 ransomware, interrupting operations through attacking the network and computing
8 infrastructure by deleting data or conducting “denial of service” attacks. As I discuss
9 later in my testimony, these threats are very real and present significant risks not
10 only to the Corporation as a whole, but to our customers as well. Defending against
11 this threat requires a complete toolkit, necessitating investments in tools, personnel,
12 training, and implementation of best practices. Critical tools include email filters,
13 firewalls, intrusion detection and prevention systems, end point protection, a modern
14 remote access infrastructure, security infrastructure including a SIEM and many
15 others. The Corporation has made and continues to make prudent investments in all
16 these areas.

17 After an initial upgrade to VOIP CISCO telephony, we have since migrated to a
18 Cloud-based call center platform called Five9, which manages inbound and
19 outbound calls in customer care, provides automated workflows and other
20 capabilities. As will be discussed in detail in Company witness Estrada’s testimony,
21 this upgrade provides improved call flows, which provides a better customer
22 experience and improved call center effectiveness when responding to spikes in call
23 volumes. Additionally, we have upgraded the Itron meter data management system

1 and the software used to keep the system current. Both of these upgrades are critical
2 components for FPUC to complete its monthly meter readings.

3 **Q. Would you please discuss some of the technology investments made to keep up**
4 **with the increased expectations of customers?**

5 A. CUC and its business units are focused on fulfilling our obligation to our customers
6 to ensure safe and reliable service, while maximizing the customer experience. To
7 fulfill that obligation, we must maintain a strong IT foundation. Our Customer
8 Service and Field Operations departments are especially dependent on high-speed
9 communications and access to information and data, so it is imperative that we keep
10 up with technology. CUC's IT function holds certain key expectations as it relates to
11 our technology infrastructure, including, among other things, the ability to achieve
12 higher availability, improved data security, and overall improvement in infrastructure
13 resilience. FPUC has continued to make the necessary investments to provide the
14 secure foundation required of technology. One of the investments CUC has made to
15 the benefit of FPUC, is in a Tier 3 data center. A Tier 3 data center is designed to
16 provide a higher uptime and redundancy for critical components of CUC's corporate
17 network. This data center is physically maintained behind several layers of limited
18 access doorway, next to a control room that is manned 24 hours per day, seven days
19 a week, all year, with camera access to monitor the room. This includes redundant
20 climate control, uninterrupted power supply, an on-site backup generator, locked
21 cabinets, and multipath data access redundancy. We have enhanced our core server
22 infrastructure in the data center by upgrading it to the Dell-EMC VxRail hyper-
23 converged appliance, which is the next generation of virtualized server environment.

1 This upgrade provides a higher level of reliability, uptime and scalability of the
2 server infrastructure. This upgrade also supports the growing data volumes required
3 for existing and growing customer base and is critical to continue providing reliable
4 services.

5 Additionally, we have setup a disaster recovery and co-location site with a third-
6 party vendor, Tierpoint, who is a leading data center provider. This site is essential
7 to providing operational continuity at a backup site in the event of a failure of our
8 primary data center. This alternative physical site ensures that our core and critical
9 applications, such as dispatch systems, will continue to operate in an emergency.
10 For further protection, FPUC has also implemented a data replication service called
11 Zerto. This system ensures that our customer and operational data is protected in the
12 event of data loss resulting from catastrophic events, such as a malicious ransomware
13 attack.

14 **Q. Would you please discuss the changes that CUC has made, since FPUC's last**
15 **rate case, as it relates to FPUC's Customer Information System ("CIS")?**

16 A. The existing CIS ("ECIS") for FPUC was migrated to a hosted solution with a third-
17 party vendor, Vertex. This third-party hosted solution also enables the Company to
18 provide a more consistent level of uninterrupted support.

19 **Q. Why was this migration necessary?**

20 A. The on-premises IBM AS400 that hosted the CIS had reached "end of life". AS400
21 mid-range systems were introduced in 1988 and have become obsolete and difficult
22 to support internally in terms of staffing and maintenance support and providing the
23 reliability and uptime requirement for a core critical system such as billing.

1 **Q. Is the Vertex system the final solution for the issues you have identified?**

2 A. No. The Corporation is currently implementing a new CIS system that is based on
3 the SAP platform. SAP is a global leader in enterprise applications and business
4 applications. We are replacing the legacy ECIS system with an advanced SAP
5 solution for our CIS and Field Service Management (“FSM”). This initiative is
6 driven by the necessity to address the obsolescence of our current platforms and to
7 significantly upgrade our field service processes.

8 This new SAP system will bring many benefits, including an enhanced customer
9 experience, by streamlining interactions and ensuring seamless service delivery. The
10 customer experience will be further bolstered by the implementation of a new
11 customer portal, making it easier for customers to access information and services.
12 We are implementing a modern field service management solution replacing a
13 manual paper-based process and aim to improve the effectiveness of our service
14 operations. The SAP FSM solution will enable better scheduling, real-time updates,
15 and more efficient resource allocation, resulting in quicker and more reliable service
16 for our customers. With cybersecurity threats becoming increasingly sophisticated, it
17 is imperative to safeguard our customer data. The new SAP solution will incorporate
18 state-of-the-art security measures to protect sensitive information and ensure
19 compliance with industry standards and regulations. In addition to enhancing
20 security, the new system will provide robust data management capabilities, ensuring
21 the integrity and confidentiality of customer information. This will build greater trust
22 and confidence among our customers. This project represents a significant
23 investment that will benefit our customers and establish a solid IT platform for the

1 Corporation's future. By adopting the latest technology, we are not only addressing
2 current challenges but also positioning ourselves for long-term success and
3 sustainability. SAP's product is a modern platform that will also include logging and
4 auditing, improved data security, and will allow us to build future capabilities.

5 The new system is scheduled to go live in August 2024 and will be followed by three
6 months of hypercare to ensure a smooth transition and address any issues that may
7 arise post-implementation. A modern billing system based on SAP RISE cloud
8 architecture brings numerous enhancements that include improved security,
9 comprehensive logging and controls and advanced functionalities designed to elevate
10 the customer experience. These features not only streamline operations but also lay
11 the groundwork for a more sophisticated and responsive customer service framework
12 in the future.

13 The additional costs for the CIS implementation are consistent with the industry
14 benchmarks as was determined during the selection process. These costs are
15 incremental and cannot be entirely offset by savings from retiring the old legacy
16 platform. The old legacy platform has lower operating costs but is inflexible and has
17 limited features. As such, it brings associated risks with reliability, inflexibility and
18 challenges with data security. Retaining the legacy platform therefore would lead to
19 higher costs in the future.

20 **Q. Why is another CIS installation necessary?**

21 A. The later version of the ECIS product from Vertex, which we are replacing, was
22 based on newer technology in 2012. This product is called ECIS+. To date, ECIS+
23 is not as mature as expected and the support from the product vendor has fallen short

1 of our expectations. Pending our anticipated future upgrade, we continue to support
2 the legacy ECIS product by making spot upgrades where possible and implementing
3 customized solutions when necessary. However, the ECIS product is an obsolete
4 product that has many deficiencies. Due to the older technology, making changes to
5 the product is difficult and expensive. The availability of support both internally and
6 externally is difficult since talent to support this product is scarce.

7 **Q. Has the Corporation made other changes in IT that ultimately benefit FPUC?**

8 A. Yes. Since the acquisition of FPUC, we have upgraded the IT organization as well as
9 the customer service organization to be able to support the implementation of a
10 modern CIS system, which is demanding in terms of internal resources and change
11 management. As mentioned earlier, we have upgraded the IT and customer service
12 organizations to add key leadership and technical positions. We are also going
13 through a rigorous process to select a modern, secure and industry-standard platform
14 by utilizing industry expertise.

15

16 **CYBER SECURITY**

17 **Q. Would you provide some background on the cyber security risk?**

18 A. Yes. Since 2013, cybersecurity has emerged as a significant concern that can
19 adversely impact all organizations and industries. Ransomware has become a
20 commercial business for threat actors, with double extortion tactics now being used
21 against organizations. In a double extortion attack, the victim's sensitive data is
22 exfiltrated in addition to encrypting the data to give the attacker additional leverage.
23 According to a report by Sonicwall, a leading provider of firewall and next

1 generation cybersecurity solutions, ransomware was up 151% in the first part of
2 2021 compared to the prior year¹.

3 The impact of ransomware is also getting costlier, with the average remediation costs
4 approaching nearly \$1.4 million in 2021, as per a report by SOPHOS, a British
5 security software and hardware company.² Threat actors have become more
6 sophisticated, better funded and their numbers have grown. Affiliate programs
7 involving cybercriminal organizations and syndicates carry out targeted attacks
8 against organizations frequently, as seen in the Colonial Pipeline ransomware attack
9 in 2021.³ The energy industry, as a key part of the country's critical infrastructure, is
10 a prime target. Advanced persistent threats have become a daily reality for energy
11 companies. Modern cybercriminals spend significant amounts of time dissecting and
12 eventually infiltrating their target, sometimes even going as far as writing custom
13 malware for the software used by the target organization. This occurred with the
14 2020 Solarigate attack in which nation-state threat actors installed malware on
15 SolarWinds software that was then passed to SolarWinds' infrastructure management
16 customers around the world. In addition, the so-called "darkweb" has become the
17 primary location where criminal organizations sell stolen corporate information,
18 personally identifiable information, or zero-day exploits to be used in future attacks -
19 - all under the cover of anonymity. The number and type of threat actors continue to
20 increase. A strong and prudent cybersecurity posture is essential to ensure
21 operational reliability and resilience to serve our customers.

¹ <https://www.sonicwall.com/medialibrary/en/infographic/2021-mid-year-update-sonicwall-cyber-threat-report.pdf>

² [The State of Ransomware 2022 – Sophos News](#)

³ <https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure>

1 **Q. Has the Company made any changes in its systems regarding cyber security?**

2 A. Yes. The three basic tenets of cyber security are confidentiality, integrity and
3 availability. We have made prudent investments around these tenets in an effort to
4 strengthen our IT technology foundation including investments in data centers, core
5 server infrastructure, and upgraded data networks. Cybersecurity concerns require
6 investments that are incremental to foundational investments. We follow industry
7 frameworks including NIST and ONG-C2M2 (Capability Maturity Model) and have
8 made investments in technology and tools, personnel, policies, employee education,
9 monitoring, and vulnerability management.

10 **Q. What other steps has the Corporation taken to improve its cyber security**
11 **environment?**

12 A. We invested in security educational tools to ensure our employees can recognize and
13 appropriately respond to the latest phishing attempts. We have also created a
14 Cybersecurity team, staffed with multiple analysts who maintain “eyes on” the
15 environment. CUC has also taken the following steps to further secure the
16 environment:

- 17 • Formed a Critical Incident Response Team as a key part of our governance;
- 18 • Deployed key technology such as email gateway and data loss prevention, which
19 secures sensitive information to provide industry leading protection;
- 20 • Procured endpoint detection & response technology to provide crucial visibility into
21 what traverses our environment;
- 22 • Engaged an industry leading company to engage in managed detection & response.
23 Managed detection and response (MDR) is an outsourced service that provides

1 organizations with threat hunting services and responds to threats once they are
2 discovered;

3 • Invested in identity and access management solutions in response to the credential
4 theft campaigns, which have accelerated over the course of the COVID-19
5 pandemic;

6 • Implemented a vulnerability management program to proactively identify
7 vulnerabilities in our enterprise. This program leverages a NIST-approved suite of
8 tools; and

9 • We are implementing key cloud-based tools to further enhance our cyber security
10 posture. This includes ZSCALER Zero trust VPN solution and Web Proxy, Darkweb
11 monitoring, Splunk SIEM and Threat intelligence product.

12 Each of these actions has benefited CUC's business units in Florida, as well as its
13 business units in other states.

14 **Q. Are there any other changes that the Company made to support the new cyber**
15 **security environment?**

16 A. Yes. FPUC has benefited from CUC's establishment of key leadership and specialist
17 positions within the Business & Information Services organization to keep up with
18 evolving technologies and capabilities. In the past 7 years, the Corporation has
19 established the following positions:

20 • Chief Information Officer, which is my current role, is part of the company
21 leadership and oversee all aspects of the IT function including governance, IT
22 operations and IT project delivery;

- 1 • Assistant Vice President of Enterprise Applications with responsibility for all
2 business applications, data analytics and IT projects;
- 3 • Director of Infrastructure with responsibility for data and voice networks, data center
4 operations and IT infrastructure operations;
- 5 • Director of Information Security with responsibility for cyber security;
- 6 • Help Desk Manager with responsibility for supporting all end users and providing IT
7 services;
- 8 • Patching administrators who ensure that all software applications and devices in the
9 Company are patched to the acceptable level and reduce vulnerability to a
10 cyberattack;
- 11 • Cyber Security analysts that report into IT monitor the network, perform triage of
12 incidents and support user education;
- 13 • Manager of IT Compliance and Control, who is a key to ensure reporting on key IT
14 controls, identifying gaps and following up on the gaps to ensure closure and
15 maintain a strong control environment;
- 16 • IT Compliance and Control Analyst to assist with the above activities.

17 The Manager and analyst positions are being added in 2024 to ensure robust
18 governance and adherence to IT General Controls (ITGC) and cybersecurity
19 standards. The positions will perform continuous gap assessments, ensuring real-
20 time identification, and mitigation of compliance issues. They will be responsible for
21 developing and tracking detailed action plans to address any identified compliance
22 gaps, ensuring timely and effective remediation.

23 The positions will cover over 30 different areas, including but not limited to:

- 1 • Patching Policy and Procedures: Ensuring all systems are updated and compliant
2 with the latest security patches.
- 3 • Event Log Management: Monitoring and managing event logs to detect and
4 respond to potential security incidents.
- 5 • Baseline Configuration Compliance: Ensuring systems are configured according
6 to approved baseline configurations to prevent security vulnerabilities.
- 7 • Privileged Access Management: Managing and monitoring privileged access to
8 critical systems to prevent unauthorized access.
- 9 • Change Management: Overseeing change management processes to ensure all
10 changes are documented, tested, and approved.
- 11 • Access Reviews: Conducting regular reviews of user access rights to ensure
12 compliance with the principle of least privilege.

13 **Q. What technology investments is the Company prioritizing in the near future to**
14 **enhance security, efficiency and overall operations?**

15 A. Our technology investment strategy is based on the objective of improving customer
16 service, protecting the business against cyber threats, securing customer data,
17 improving IT controls through IT service management modernization and improving
18 core administrative and operational processes through an enterprise-wide Enterprise
19 Resource Planning (ERP) system that will integrate with the CIS system being
20 implemented.

21 Second, we're upgrading our IT Service Management infrastructure. This
22 investment will bolster our asset discovery capabilities, streamline patch

1 management, and strengthen overall IT controls, ultimately enhancing our customer
2 service quality.

3 Additionally, we're initiating the implementation of a comprehensive ERP system.
4 This will replace outdated, difficult-to-support platforms that pose potential security
5 risks. The new ERP system will integrate and streamline our core finance, project
6 management, asset management, and procurement processes. Beyond operational
7 efficiencies, this investment is expected to optimize our workforce needs and reduce
8 future costs.

9 These initiatives form the core of our technology modernization program, designed
10 to fortify our security posture, increase operational efficiency, and deliver reliable
11 service to our customers.

12 **Q. Have the investments in the IT function been prudent?**

13 A. Yes, absolutely. As I have described, they have been necessary and prudent to stay
14 current with technology advancement in a number of areas and to protect our
15 systems, and customers, from sophisticated cyberattacks by a wide variety of bad
16 actors.

17 **Q. Does this conclude your testimony?**

18 A. Yes.

Witness Vikrant Gadgil's MFRs

SCHEDULE	TITLE	WITNESS
C-7, page 8 of 8 C-41	Over and Under Adjustments (Accts. 920,921,923) O&M Benchmark Variance by Function	Gadgil Gadgil (input support)

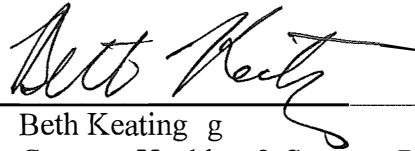
Docket No. 20240099-EI
Florida Public Utilities

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing filing has been served by Electronic Mail this 22nd day of August, 2024, upon the following:

Walter Trierweiler, Public Counsel
Office of the Public Counsel
c/o The Florida Legislature
111 West Madison St., Rm 812
Tallahassee, FL 32399-1400
Trierweiler. walt@leg.state.fl.us

By: _____



Beth Keating g
Gunster, Yoakley & Stewart, P.A.
215 South Monroe St., Suite 601
Tallahassee, FL 32301
(850) 521-1706