



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

May 24, 2022

**BY E-FILING**

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

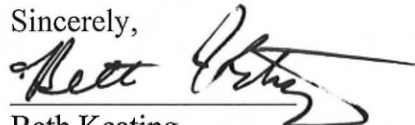
**Re: Docket No. 20220067-GU: Petition for rate increase by Florida Public Utilities Company, Florida Division of Chesapeake Utilities Corporation, Florida Public Utilities Company - Fort Meade, and Florida Public Utilities Company - Indiantown Division.**

Dear Mr. Teitzman:

Attached, for electronic filing, please find the Testimony and Exhibit VG-1 of Vik 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 10 of 27)

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. 20220067-GU: Petition for rate increase by Florida Public Utilities Company,  
3 Florida Division of Chesapeake Utilities Corporation, Florida Public Utilities Company -  
4 Fort Meade, and Florida Public Utilities Company - Indiantown Division.

5 Prepared Direct Testimony of Vikrant Gadgil

6 Date of Filing: May 24, 2022

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

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

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

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

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

18 A. The IT function team is staffed by approximately 34 employees and is responsible  
19 for the holistic, complete support of around 1000+ employees, multiple contractors,  
20 all 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, customer data security, enabling data  
23 analytics tools and services, supporting business applications across all corporate  
24 functions, including, but not limited to: billing, financial systems, work order

1 management, human resource information systems, geographic information systems,  
2 Outage Management, email, and office productivity tools.

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

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

9 I have over 25 years of experience in the IT industry. I hold a Bachelor of  
10 Engineering degree in Electrical Engineering from National Institute of Technology,  
11 India and an MBA from Indian Institute of Management – Calcutta India.

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

13 A. When referring to the Florida Local Distribution Company business units (i.e.,  
14 Florida Public Utilities Company (Natural Gas Division), Florida Public Utilities  
15 Company-Fort Meade, Florida Public Utilities Company-Indiantown Division, and  
16 the Florida Division of Chesapeake Utilities Corporation d/b/a Central Florida Gas),  
17 I will refer to these entities collectively as “FPUC” or “the Company”. When  
18 referring to Chesapeake Utilities Corporation, the parent company, I will refer to it as  
19 “CUC” or the “Corporation.”

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

22 A. No, I have not.

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

1 A. No, I have not.

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

3 A. My testimony will discuss the following topics.

4 (i) Technology advancements implemented since the acquisition of FPUC by CUC.

5 (ii) Planned new technology implementation.

6 (iii) Improvements in cyber security.

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

8 A. Attached as Exhibit VG-1 is a list of Minimum Filing Requirements that I co-  
9 sponsored.

10 **IT SERVICE LEVELS**

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

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

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

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

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

14

15          **TECHNOLOGY ADVANCEMENTS**

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

18          A.    Digital transformation is critical to the core operations of all CUC's business units.  
19          CUC is constantly investigating new ways to incorporate the power of data and  
20          communications technology to improve services and increase efficiency for our  
21          customers. Over the past 10 to 15 years, the key technology developments impacting  
22          CUC and its businesses have involved the expansion of mobile computing, the  
23          emergence of smartphones, network upgrades, enhanced social media and an  
24          expanded number of platforms, predictive analytics, and hyper-converged

1 infrastructure. In addition, our bandwidth requirements on wireless and wide area  
2 networks have increased to keep 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, 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 risk not only  
10 to the Corporation as a whole, but to our customers as well. Defending against this  
11 threat requires a complete toolkit, necessitating investments in tools, personnel and  
12 implementation of best practices. Critical tools include email filters, firewalls,  
13 intrusion detection and prevention systems, end point protection and many others.  
14 The Corporation has made prudent investments in all these areas.  
15 We have also upgraded the Voice Over Internet Protocol or VOIP communication  
16 system to CISCO telephony, which is at the core of our customer call center. As will  
17 be discussed in detail in witness Parmer’s testimony, this upgrade provides improved  
18 call flows, which provides a better customer experience and improved call center  
19 effectiveness when responding to spikes in call volumes. Additionally, we have  
20 upgraded the Itron meter data management system and the software used to keep the  
21 system current. Both of these upgrades are critical components for FPUC to  
22 complete its monthly meter reading.

23 **Q. Would you please discuss some of the technology investments made to keep up**

1           **with the increased expectations of customers?**

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

1 for existing and growing customer base and is critical to continue providing reliable  
2 services.

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

12 **Q. Would you please discuss the changes that CUC has made as it relates to**  
13 **FPUC’s Customer Information Systems (“CIS”)?**

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

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

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

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



1 A. No. The Corporation is currently evaluating a newer CIS system and we anticipate  
2 filing a separate petition at some future point to address it. The Company is not  
3 proposing approval of any future CIS system as a part of this rate proceeding.

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

5 A. This later version of the ECIS product from Vertex, was based on newer technology  
6 in 2012. This product is called ECIS+. To date, ECIS+ is not as mature as expected  
7 and the support from the product vendor fell short of our expectations. Pending our  
8 anticipated future upgrade, we continue to support the legacy ECIS product by  
9 making spot upgrades where possible, and implementing customized solutions when  
10 necessary.

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

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

19 **CYBER SECURITY**

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

21 A. Yes. Since 2008, cybersecurity concerns have emerged as a significant concern that  
22 can adversely impact all organization and industries. Ransomware has become a  
23 commercial business for threat actors, with double extortion tactics now being used

1 against organizations. In a double extortion attack, the victim’s sensitive data is  
2 exfiltrated in addition to encrypting the data to give the attacker additional leverage.  
3 According to a report by Sonicwall, a leading provider of firewall and next  
4 generation cybersecurity solutions, ransomware was up 151% in the first part of  
5 2021 compared to the prior year<sup>1</sup>.

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

---

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

<sup>2</sup> [The State of Ransomware 2022 – Sophos News](#)

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

1 cover of anonymity. The number and type of threat actors continue to increase. A  
2 strong and prudent cybersecurity posture is essential to ensure operational reliability  
3 and resilience to serve our customers.

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

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

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

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

- 20 • A Critical Incident Response Team was formed and is a key part of our governance.  
21 • Deployed key technology such as email gateway and data loss prevention which  
22 secures sensitive information to provide industry leading protection.

1 • Procured endpoint detection & response technology to provide crucial visibility into  
2 what traverses our environment.

3 • Engaged an industry leading company to engage in managed detection & response.  
4 Managed detection and response (MDR) is an outsourced service that provides  
5 organizations with threat hunting services and responds to threats once they are  
6 discovered.

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

10 • Implemented a vulnerability management program to proactively identify  
11 vulnerabilities in our enterprise. This program leverages a NIST-approved suite of  
12 tools.

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

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

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

21 • Chief Information Officer, which is my current role, is part of the company  
22 leadership and oversee all aspects of the IT function including governance, IT  
23 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 **Q. Have the investments in the IT function been prudent?**

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

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

19 A. Yes.

**SCHEDULE**

**TITLE**

**Witness**

**PROJECTED TEST YEAR**

G2-19 a to d	Projected Test Year - Calculation of Operation and Main Expense Supplement	M. Cassel, J. Bennett, M. Galtman, V. Gadgil, M. Napier, K. Parmer, N. Russell, K. Lake, D. Rudloff, B. Hancock
G2-19f	Over and Under Adjustments	M. Cassel, J. Bennett, M. Galtman, V. Gadgil, M. Napier, K. Parmer, N. Russell, K. Lake, D. Rudloff, B. Hancock