FILED
November 9, 2026
Missouri Public
Service Commission

Exhibit No. 39

Evergy Missouri Metro – Exhibit 39
Direct Testimony of Gary Johnson
Case No. ER-2026-0143

Exhibit No.:	
Issue:	Cyber Tracker
Witness:	Gary Johnson
Type of Exhibit:	Direct Testimony
Sponsoring Party:	Evergy Missouri Metro
Case No.:	ER-2026-0143
Date Testimony Prepared:	February 6, 2026

MISSOURI PUBLIC SERVICE COMMISSION

CASE NO.: ER-2026-0143

DIRECT TESTIMONY

OF

GARY JOHNSON

ON BEHALF OF

EVERGY MISSOURI METRO

Kansas City, Missouri

February 2026

DIRECT TESTIMONY

OF

GARY JOHNSON

Case No. ER-2026-0143

I. INTRODUCTION

Q: Please state your name and business address.

A: My name is Gary Johnson. My business address is 1200 Main St Kansas City Missouri 64105.

Q: By whom and in what capacity are you employed?

A: I am employed by Evergy Metro, Inc. and serve as Senior Director, Information and Cyber Security for Evergy Metro, Inc. d/b/a as Evergy Missouri Metro ("Evergy Missouri Metro"), Evergy Missouri West, Inc. d/b/a Evergy Missouri West ("Evergy Missouri West"), Evergy Metro, Inc. d/b/a Evergy Kansas Metro ("Evergy Kansas Metro"), and Evergy Kansas Central, Inc. and Evergy South, Inc., collectively d/b/a as Evergy Kansas Central ("Evergy Kansas Central") the operating utilities of Evergy, Inc. ("Evergy").

Q: On whose behalf are you testifying?

A: I am testifying on behalf of Evergy Missouri Metro ("Evergy Missouri Metro," "EMM," or the "Company").

Q: What are your responsibilities?

A: I have responsibility for IT/OT Infrastructure and Security. Infrastructure includes (architecture, data centers, computer and storage, network, telecommunications, end user support, etc.) and security includes (security operations, incident response, governance and compliance, access management, physical secutiy, etc.) This does not include any security

responsibilities for Operations Technology at the nuclear power plant, those are managed at the plant level.

Q: Please describe your education, experience, and employment history.

A: I am a US Army veteran. I studied Computer System Administration in college and have been working in technology functions for over 40 years. I have spent the last ten years in my current role at Evergy. Prior to this role I ran the security (cyber and physical) organization for Cerner Corporation, a healthcare software company in Kansas City.

Q: Have you previously testified in a proceeding at the Missouri Public Service Commission ("PSC" or "Commission") or before any other utility regulatory agency?

A: No.

Q: What is the purpose of your direct testimony?

A: The purpose of my testimony is to discuss and support EMM's request for a Critical Infrastructure Protection ("CIPS")/Cyber Security Tracker (collectively the "Tracker").

II. CYBER TRACKER

Q: What is the purpose of the Tracker?

A: The purpose of the Tracker is to permit recovery of incremental non-labor operations and management costs incurred to meet regulatory requirements for protection of the Company's critical infrastructure. As I am sure you know, US critical infrastructure has been under siege for the last few years. The Russians successfully infiltrated nuclear networks (including Wolf Creek) in 2017. Chinese attackers have been able to infiltrate large US based carrier networks. Evergy needs to be able to make quick changes to its security environments and needs to be able to recover the expenses related to those changes

as they occur or risk exposing the grid to nation state attackers. This could jeopardize the delivery of power and the protection of customer data.

Q: Why is the Company requesting a cyber tracker?

A: The Company fully anticipates that the cyber security operations and management expense will increase substantially over the next few years. And, more importantly, in emergency situations, EMM will need to be able to respond quickly and with flexibility to new threats surfacing every day. The Tracker permits EMM flexibility because cyber security and critical infrastructure costs are unpredictable and can vary from amounts established in base rates. Moreover, the Company is including the addition of a security component to the Tracker because security threat costs are expected to have a significant impact on the Company. The Company has had to bring in outside security consultants multiple times in the last 24 months to help ensure that the networks were clean when nation state attackers had compromised third parties (F5 and SolarWinds are recent examples) and when Volt Typhoon (Chinese) had infiltrated a Company switch. Most security tools are now subscription based which makes them an O&M charge. Without the flexibility of the Tracker EMM will sometimes be faced with delaying or foregoing security purchases.

The Company's request for the Tracker is in the public interest and necessary to ensure that it is able to provide safe and adequate service to EMM's customers at just and reasonable rates. For the reasons discussed herein, Evergy Missouri Metro is requesting that the CIP/Cyber Security Tracker be authorized by the Commission.

Q: Please describe the cyber security landscape.

A: The security threat landscape continues to increase and evolve. Critical infrastructure—the electric grid at all voltage levels—is a rich target for United States' adversaries. In addition,

there have been increases in violent domestic attacks on the nation's critical infrastructure. While EMM has been responsive to compliance with regulations, reporting, and risk-based prudent security measures, the ever-changing attack surface requires the Company to be flexible and expeditiously deploy prudent security response measures to protect the assets that serve the Company's customers.

Q: What are some of the considerations beyond compliance regulations?

A: Physical security of widely dispersed unmanned assets is a challenge. While regulations may speak to the risk and protection of these assets, the current threat landscape reinforces the need for additional reasoned and prudent investments, and additional security measures. EMM needs to increase its third-party protection services coverage to improve the ability to respond to theft and vandalism activities at Service Centers and Substations.

In addition to this, the electric industry is experiencing increased risk through supply chain sources, such as embedded cyber technology (chips, malware, backdoors, etc.) in electrical equipment installed by nation-state adversaries. While regulations exist to address each of these issues, compliance is representative of the security baseline or floor. Reasonable layered security controls represent the most effective way to protect assets that serve EMM's customers. Another risk that continues to promulgate across all industries and entities is ransomware attacks, such as the one with Colonial Pipeline in May 2021 that disrupted oil supply for five days primarily in the southeastern United States. These types of attacks are very costly and disruptive to businesses and customers.

Q: In what ways do advancements in artificial intelligence ("AI") impact the Company's cyber security risk profile and the security of the electrical grid?

A: Attackers are using AI enhanced tools to focus attacks on users with privileged credentials. Once an attacker obtains those credentials, they can often further expand that access into critical parts of an environment. This can lead to customer data exposure and the potential of cyber caused outages to the GRID.

Q: Is Evergy Missouri Metro subject to these risks?

A: Yes, EMM, like all entities with connectivity to the internet, is subject to any and all cyber security threat. The Company has deployed a layered defense strategy to address these threats. This defense strategy is constantly under stress by potential attackers looking for a way to breach the environment.

Q: How does the Company's investments in critical infrastructure and cyber security operations and management benefit customers?

A: To ensure reliability of systems and electrical service, EMM needs to anticipate service disruptions and have processes in place to anticipate issues, root cause analysis tools, and response tools for recovery/restoration of service. Similar to service disruptions by weather, the Company has been working to anticipate disruptions from threat actors whether that is a local threat hacking into networks for personal gain or a nation state with intent to harm the United States infrastructure. EMM's ability to deploy security measures in an efficient and reasonable manner is critical to keeping the lights on. In addition, because of the pandemic and the slowing of global supply chains, certain equipment has much longer lead times than historical experience. Destruction of equipment by bad actors, coupled with the inability to respond quickly with new equipment, could extend restoration

times significantly. The Company has spare equipment and response plans to prepare for outage restoration. Whether required by storms or breaches of security measures, EMM has the same goal – ensure customer service is restored promptly.

Q: Broadly stated, what is the impact to the Company with respect to security?

A: Security continues to be a top priority for the Company. EMM is committed and required to comply with standards set out to establish a baseline and floor for protection of the electric grid and EMM's assets. In addition to compliance with regulations, the Company takes additional steps to ensure a layered defense posture or "defense in depth" and prudent mitigation of risk to manage exposure to the evolving security threat landscape. The security measures are necessary to ensure EMM is positioned to reliably provide services to customers given the evolving and increasing threats to the United States and its critical infrastructure. The costs of compliance with regulations and being responsive to prudent security measures are constantly changing and are expected to be substantial. The Company has already committed significant resources to ensuring the security of its assets, customers, and personnel. Going forward, the dedication of resources and efforts will continue and will be increasing.

Q: What is the Company requesting regarding the security portion of the Tracker in this case?

A: Evergy Missouri Metro requests the Commission authorize the CIPS/Cyber Security Tracker and, in addition, add a security component to ensure recovery of the costs necessary to respond to evolving threats, new reporting requirements that are expected to be mandated in the near term, and additional government-mandated regulations regarding security of assets—both physical and cyber—essential to the safe and reliable operation of

the Company's assets. These requirements are expected to affect all EMM's infrastructure regardless of voltage.

Q: What is the cost for security to the Company?

A: The costs to secure EMM's assets and comply with existing regulations and increasing requirements have the potential to be substantial. The Company has a cost plan for security spend as it exists today. However, EMM will need the ability to be agile and responsive to emerging threats as well as new requirements and regulations.

Q: Why are these costs in addition to the Company's costs to comply with regulations?

A: Compliance is designed at a specific "point in time." Attackers are continuously evolving their attack methods and EMM needs to be able to quickly adapt to the new approaches. As mentioned previously in this testimony, compliance is often defined at the floor of what may be needed for security. There are security events that require EMM to respond with third party evaluations or additional security measures to protect the Company's assets and people. These responses are above and beyond compliance with baseline regulations and are necessary to meet our service obligations to our customers. The associated costs are prudently incurred and would be appropriately recovered through the proposed CIPS/Cyber Security Tracker.

Q: Is this request asking for unlimited spending for security costs?

A: No. EMM has discussed compliance requirements of Department of Energy ("DOE"), the Federal Regulatory Energy Commission ("FERC") and the North American Electric Reliability Corporation's ("NERC") that are targeted at security. The mandates for reporting and partnerships continue to grow and are coming from other federal agencies. In addition to FERC and NERC compliance mandates, EMM has increasing security

requirements coming from numerous federal agencies and departments that are in the process of taking shape. The Company is asking the Commission to authorize it to add these categories to the CIPS/Cyber Security Tracker for these types of costs. The costs will include the addition of personnel, substantial physical security measures, computer software enhancements and support, and the development of new programs to address the hardening of the Company's infrastructure. As discussed by EMM witness Mr. Klote, the Company will use specific accounting treatment through specific general ledger codes, as it has in the past, to track all costs associated with each specific effort responsive to appropriate security measures for reporting, partnerships, and the Company's asset protection. The Company will track these costs for consideration for recovery in the next rate proceeding when the costs would be reviewed by the Staff of the Commission.

Q: Does the requested security tracker include internal labor costs?

A: It does not include internal labor costs for current employees. It does accommodate a need for additional personnel with enhanced security skills to work on emerging security technologies and to interface with state and federal government agencies to promote partnerships for the security of Missouri and EMM's customers.

Q: If the Commission approves the CIPS/Cyber Security Tracker, what is the base level of costs included in the revenue requirement in this case?

A: As discussed further by Mr. Klote, the base level included in the revenue requirement for EMM is $4,492,878.

III. CONCLUSION

Q: Please summarize your testimony.

A: Due to the increased risks associated with cyber security, EMM is requesting the Commission approved a CIPS/Cyber Security Tracker which would permit recovery of incremental costs incurred to meet regulatory requirements for protecting the Company from cyber threats. Because attackers are becoming more sophisticated, and the cyber security landscape continues to evolve, EMM expects cyber security expenses will increase. The requested CIPS/Cyber Security Tracker ensures EMM has the flexibility to respond quickly to deploy prudent security measures to protect the assets that serve customers. The request for the Tracker is in the public interest and necessary for EMM to provide safe and adequate serve customers.

Q: Does that conclude your testimony?

A: Yes, it does.

BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of Evergy Metro, Inc. d/b/a Evergy Missouri Metro's Request for Authority to Implement A General Rate Increase for Electric Service	))))	Case No. ER-2026-0143

AFFIDAVIT OF GARY JOHNSON

STATE OF MISSOURI)
) ss
COUNTY OF JACKSON)

Gary Johnson, being first duly sworn on his oath, states:

1. My name is Gary Johnson. I work in Kansas City, Missouri and I am employed by Evergy Metro, Inc. as Senior Director, Information and Cyber Security.

2. Attached hereto and made a part hereof for all purposes is my Direct Testimony on behalf of Evergy Missouri Metro consisting of nine (9) pages, having been prepared in written form for introduction into evidence in the above-captioned docket.

3. I have knowledge of the matters set forth therein. I hereby swear and affirm that my answers contained in the attached testimony to the questions therein propounded, including any attachments thereto, are true and accurate to the best of my knowledge, information and belief.

Gary Johnson

Subscribed and sworn before me this 6th day of February 2026.

Notary Public

My commission expires: April 26, 2029

ANTHONY R WESTENKIRCHNER
NOTARY PUBLIC - NOTARY SEAL
STATE OF MISSOURI
MY COMMISSION EXPIRES APRIL 26, 2029
PLATTE COUNTY
COMMISSION #17279952