Exhibit No.:
Issue: Cyber Tracker
Witness: Charles King
Type of Exhibit: Direct Testimony
Sponsoring Party: Evergy Missouri West
Case No.: ER-2027-0077
Date Testimony Prepared: November 3, 2026

MISSOURI PUBLIC SERVICE COMMISSION

CASE NO.: ER-2027-0077

DIRECT TESTIMONY

OF

CHARLES KING

ON BEHALF OF

EVERGY MISSOURI WEST

Kansas City, Missouri

November 2026

DIRECT TESTIMONY

OF

CHARLES KING

Case No. ER-2027-0077

I. INTRODUCTION

Q: Please state your name and business address.

A: My name is Charles King. 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 Vice President, Chief Technology Officer for Evergy Metro, Inc. d/b/a Evergy Missouri Metro ("EMM") and Evergy Metro, Inc. d/b/a Evergy Kansas Metro ("EKM") (collectively, "Evergy Metro"), Evergy Missouri West, Inc. d/b/a Evergy Missouri West ("EMW" or "Company"), and Evergy Kansas Central, Inc. and Evergy Kansas South, Inc., collectively d/b/a Evergy Kansas Central ("EKC") the operating utilities of Evergy, Inc.

Q: On whose behalf are you testifying?

A: I am testifying on behalf of Evergy Missouri West.

Q: What are your responsibilities?

A: As Chief Technology Officer at Evergy I have responsibility for all IT and security functions spanning corporate, customer, and operations applications, cyber and physical security, and corporate infrastructure including network, Evergy data centers, telephony, field communications, enterprise architecture, project management, testing, help desk, and desktop support.

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

A: I hold B.S. and M.S. degrees in industrial engineering from the University of Arkansas, and B.S. in mathematics from Harding University with now more than 30 years of experience leading large-scale IT and technology functions spanning technology consulting, telecommunications, media/entertainment, and electric utilities encompassing large-scale modernizations, mergers and acquisitions, advanced technology adoption, and critical infrastructure cybersecurity. My career began with Andersen Consulting (now Accenture) followed by leadership roles at Sprint, Embarq, CenturyLink/Lumen, and Dish Network prior to Evergy.

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: Yes. I have previously testified at the Commission.

Q: What is the purpose of your direct testimony?

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

II. CIPS/CYBER SECURITY TRACKER

Q: Why is the Company requesting a Tracker for CIPS/cyber security costs?

A: Our levels of spending at Evergy on security have been fairly steady in past years due largely to the timing of multi-year licensing agreements and those costs being amortized over the life of the agreement. However, the security landscape is changing. The Company fully anticipates that security operations and management expense will increase substantially over the next few years. And, more importantly, in emergency situations, EMW will need to be able to respond quickly and with flexibility to new threats surfacing

every day. Security and critical infrastructure costs are unpredictable and can vary from amounts established in base rates. The flexibility provided by a Tracker will allow EMW to act quickly and make necessary purchases to ensure its critical infrastructure remains safeguarded from physical and cyber threats.

Evergy Missouri West is requesting that the CIP/Cyber Security Tracker be authorized by the Commission. 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 EMW's customers.

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 an owner and operator of critical infrastructure, it is imperative that Evergy is nimble in the deployment and management of its security resources, making changes or improvements as necessary to combat the growing threat posed by cyber and physical security attacks. Evergy must be empowered to respond to ever-evolving threats to ensure the continuous delivery of power and protect customer data. Most security tools are now subscription based which makes them an Operations and Management ("O&M") expense. The recovery of expenses associated with security resources is appropriate because those resources are used to mitigate risks posed by nation state attackers and such attacks could greatly impair or prohibit Evergy from providing power to its customers.

Q: Please describe the threat landscape facing utilities today.

A: Critical infrastructure—the electric grid at all voltage levels—is a rich target for United States' adversaries. US critical infrastructure has been under siege from both physical and cyber security threats for the last few years as the threat landscape continues to increase and evolve.

Physical security of widely dispersed unmanned assets is a challenge. The U.S. electric grid has faced growing security issues from physical threats, including vandalism, assault of utility workers, intrusion of property, and theft of components, like copper wiring.[1] There have also been increases in violent domestic attacks on the nation's critical infrastructure. One recent attack in California on two electric utility transformers resulted in a power outage to thousands of customers.[2] An attack in North Carolina led to days of power outages after two utility substations were shot.[3] Authorities also recently intercepted an individual who was planning to bomb a Tennessee electric substation.[4]

Like physical security threats, cyber security threats to critical infrastructure have only increased in recent years. The Russians successfully infiltrated nuclear networks in 2017.[5] Chinese attackers have been able to infiltrate large US based carrier networks.[6] 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

[1] Julia Tilton, *Rising Attacks on Power Grids Push Utilities to Prepare*, IEEE Spectrum, Mar. 16, 2026.
[2] *Man charged with blowing up PG&E transformers in California*, Associated Press, Mar. 6, 2023.
[3] Hannah Schoenbaum, *North Carolina blackouts caused by shootings could last* days, Associated Press, Dec. 5, 2022.
[4] Jonathan Mattise, *Man pleads guilty to charges that he meant to blow up a Nashville power site with a bomb-laden drone*, Associated Press, Sep. 9, 2025.
[5] Colleen Long, *Russian hackers used phishing tools in 2017 attack on grid*, Associated Press, Jul. 25, 2018.
[6] Aamer Madhani, *White House says at least 8 US telecom firms, dozens of nations impacted by China hacking campaign*, Associated Press, Dec. 4, 2024.

compromised third parties (F5[7] and SolarWinds[8] are recent examples) and when Volt Typhoon infiltrated a Company router switch, which did not result in any compromise of network traffic. 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. 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.

The current threat landscape reinforces the need for additional reasoned and prudent investments, and additional security measures. EMW 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.

While EMW has been responsive to compliance with regulations, reporting, and risk-based prudent security measures, compliance with those regulations represents the security baseline or floor. The ever-changing attack surface requires the Company to also remain flexible and expeditiously deploy prudent security response measures to protect the assets that serve the Company's customers as threats evolve. Reasonable layered security controls represent the most effective way to protect assets that serve EMW's customers.

[7] A.J. Vicens and Raphael Satter, *Breach at US-based cybersecurity provider F5 blamed on China, sources say*, Reuters, Oct. 17, 2025.
[8] Alan Suderman, *AP sources: SolarWinds hack got emails of top DHS officials*, Associated Press, Mar. 29, 2021.

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: While there are always dynamic factors in play related to cyber security, be it trends in threats or breaches, or changes to industry-specific NERC-CIP security requirements, AI represents a step change of uncertainty as we go forward. In the 12 years that I have been responsible for cybersecurity at Evergy, we have never faced a time of such uncertainty with the dynamic nature of AI and the implications to cybersecurity. Advanced AI models can now autonomously identify previously unknown vulnerabilities and develop attack techniques against them, dramatically increasing the speed and scale of cyber threats. This strengthens the longstanding reality that cyberattacks are not a question of if, but when. Evergy, along with other companies, will be required to make an unknown and unpredictable amount of investment to address these risks.

While leading technology providers are leveraging AI to identify vulnerabilities and issue security patches at unprecedented rates, many other risks remain. Vulnerabilities arising from unpatched products, legacy systems, custom configurations, and company-specific architectures cannot be broadly addressed and often require direct investment and remediation by the company. As AI continues to enhance both the frequency and sophistication of attacks, cybersecurity investments will increase and remain critical to reducing operational and business risk. Attackers are also using AI to enhance social engineering 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.

The ever-evolving nature of AI and how it is used to advance cyber security threats requires EMW to remain nimble. EMW must have the flexibility to react quickly to emerging threats and deploy resources to combat or otherwise mitigate such risks, and thus ensure the continued provision of safe and adequate service to its customers. The Tracker provides EMW that flexibility, aiding EMW in its duty to maintain grid security and keep the lights on despite AI's contribution to an evolving and increasing threat landscape.

Q: Is Evergy Missouri West subject to these risks?

A: Yes. EMW, like all entities with connectivity to the internet, is subject to any and all cyber security threats. 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 do the Company's investments in critical infrastructure and cyber security operations and management benefit customers?

A: To ensure reliability of systems and electrical service, EMW 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. In addition, since 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. While the Company has spare equipment and response plans to prepare for outage restoration.

EMW's continued ability to deploy evolving security measures in response to evolving threats, in an efficient and reasonable manner, is critical to keeping the lights on.

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. EMW is committed and required to comply with standards set out to establish a baseline and floor for protection of the electric grid and EMW'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 EMW 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 West 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 physical and cyber assets. These requirements are expected to affect all EMW's infrastructure regardless of voltage.

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

A: The costs to secure EMW'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, EMW 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 EMW 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 EMW 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. EMW has discussed compliance requirements of Department of Energy ("DOE"), the Federal Energy Regulatory 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, EMW 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 EMW 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: 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 EMW is $1,141,941.

III. CONCLUSION

Q: Please summarize your testimony.

A: Because of the increased risks associated with cyber security, EMW is requesting the Commission approve a CIPS/Cyber Security Tracker which would permit recovery of incremental costs incurred to ensure continued protection of Evergy's critical infrastructure from cyber and physical security threats. The attackers are becoming more sophisticated, and the cyber security landscape continues to evolve as AI and computer technologies continue to advance. Given this, EMW expects cyber security expenses will increase. The requested CIPS/Cyber Security Tracker ensures EMW 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 EMW to continue the provision of safe and adequate service to 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 Missouri West, Inc. d/b/a Evergy Missouri West's Request for Authority to Implement A General Rate Increase for Electric Service	))))	Case No. ER-2027-0077

AFFIDAVIT OF CHARLES KING

STATE OF MISSOURI)
) ss
COUNTY OF JACKSON)

Charles King, being first duly sworn on his oath, states:

1. My name is Charles King. I work in Kansas City, Missouri, and I am employed by Evergy Metro, Inc. as Senior Vice President, Chief Technology Officer.

2. Attached hereto and made a part hereof for all purposes is my Direct Testimony on behalf of Evergy Missouri West consisting of eleven (11) 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.

Charles King

Subscribed and sworn before me this 3rd day of November 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