BEFORE THE

PUBLIC UTILITIES COMMISSION OF OHIO

THE DAYTON POWER AND LIGHT COMPANY

CASE NO. 18-1875-EL-GRD
18-1876-EL-WVR
18-1877-EL-AAM

Distribution Modernization Plan

DIRECT TESTIMONY OF JEFFREY K. FULLER

- □ MANAGEMENT POLICIES, PRACTICES, AND ORGANIZATION
- □ OPERATING INCOME
- □ RATE BASE
- □ ALLOCATIONS
- □ RATE OF RETURN
- □ RATES AND TARIFFS
- ■ OTHER

ON BEHALF OF

THE DAYTON POWER AND LIGHT COMPANY

TABLE OF CONTENTS

I. INTRODUCTION

Q. Please state your name and business address.

A. My name is Jeffrey K. Fuller. My business address is 1900 Dryden Road, Dayton, Ohio 45439.

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

A. I am employed by AES US Services, LLC ("AES Services") as the Director of Infrastructure Security.

Q. How long have you been in your present position?

A. I assumed my present position in April 2012. Prior to that time, I worked as the Senior Security Manager (since 2007) overseeing physical security, cybersecurity, and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection ("CIP") compliance for the Dayton Power and Light Company ("DP&L").

Q. What are your responsibilities in your current position?

A. I currently lead the Infrastructure Security Organization for The AES Corporation serving as the US Operations chief security executive, and am responsible for designing, implementing, and managing the Company-wide program for protecting the Company's Operational Technology ("OT") networks, facilities, personnel, property, and assets. My organization encompasses cybersecurity functions wholly supporting the "OT" networks NERC CIP Program, all physical security functions (protection, investigations, access control, etc.), along with SOX (IT General Controls) testing, Business Continuity

Coordination, Incident Management and Emergency Response for the transmission, distribution and generation assets across the AES business portfolio, including DP&L.

Q. Will you describe briefly your educational and business background?

A. I joined DP&L in 2007 to build a then non-existent cybersecurity and NERC CIP program. Previously, following military service as an Infantryman, I spent 11 years as a police officer serving in a variety of capacities including narcotics, patrol operations, investigations, and supervision, culminating in my appointment as Police Chief. After leaving law enforcement I joined a Technology Training Company where I served as the Network Operations Manager and Technical Instructor earning numerous certifications including the Certified Information Systems Security Professional ("CISSP") and the Microsoft Certified Systems Engineer ("MCSE") certifications. I have a Bachelor of Science in Management Information Systems from Western Governor's University, and am a graduate of Northwestern University School of Police Staff and Command. I am active in the electric industry Cybersecurity and Physical Standards developments serving on the NERC Critical Infrastructure Protection Committee ("CIPC") as a voting member from the Reliability First region since 2010 and am currently serving as the Chair of the CIPC Executive Team Sub-committee focusing on CLOUD Technology within NERC CIP.

Q. What is the purpose of this testimony?

A. The purpose of this testimony is to describe the physical and cyber security measures that DP&L will implement as part of its Distribution Modernization Plan ("DMP").

II. PHYSICAL AND CYBER SECURITY

Q. Please describe the status of physical and cyber security measures as they exist now at DP&L.

A. AES's Security organization provides cybersecurity, physical security and NERC CIP compliance services for the transmission, distribution, and corporate operations of DP&L. The protection of assets, technology and processes for the DMP is managed by the Security Teams of AES. Policies dictate the tactics, techniques and procedures used by the organization to keep customer data and the overall DMP implementation secure. DP&L's cybersecurity, physical security and NERC CIP compliance policies are determined by business needs, regulatory compliance, risk assessments and industry best practices. This model reflects DP&L's goal of continuing to deliver safe and reliable service.

DP&L takes a vigilant approach as it relates to cybersecurity of its systems, applications, and networks, particularly as it relates to real-time systems such as Supervisory Control and Data Acquisition ("SCADA") systems.

Q. Does DP&L plan to implement additional physical and cyber security measures associated with its DMP?

A. Yes. Based upon guidance and expectations outlined in the Commission's PowerForward Roadmap to Ohio's Electricity Future, DP&L intends to participate in and align with recommendations of the PowerForward Data and the Modern Grid Workgroup ("DWG").

DP&L's DMP has four core projects planned pertaining to Physical and Cybersecurity for the DMP, as outlined below:

DMP Security Project One: Physical Protection

DP&L will implement physical security technologies to prevent, detect and contain malicious or unauthorized access to DP&L's DMP equipment. Those measures will include physical access control systems, camera systems, heat and motion sensors, fencing, lighting, and/or alarm monitoring technology. Equipment deployed will be monitored 24/7/365 by a team of security operators who coordinate incident response, investigations, and protection activities.

DMP Security Project Two: Data Protection

DP&L will implement a robust cybersecurity architecture to protect DP&L's investment in the DMP while using on-premise and cloud-based solutions for enhanced cybersecurity operations. Such cybersecurity technologies will include Cyber Security as a Service ("CSaaS"), Managed Security Service Providers ("MSSPs"), Network as a Service ("NaaS"), and/or cloud-based cybersecurity platforms. In addition, traditional technologies such as advanced persistent threat ("APT") appliances, firewalls, intrusion prevention systems ("IPS"), anti-virus and anti-malware will be used. Governance and guidance shall be based on industry-accepted security frameworks such as the Department of Energy ("DoE") Electricity Subsector Cyber-security Capabilities Maturity Model ("ES-C2M2"), the National Institute of Standards and Technology ("NIST") Framework, elements of the Payment Card Industry-Data Security Standard

("PCI-DSS") Framework, the System Administration, Networking and Security Institute ("SANS Institute") "Top 20," International Organization for Standardization ("ISO") 27000 and United States Computer Emergency Readiness Team ("US CERT") recommendations for security computing environments.

DP&L will securely maintain the data collected by smart meters, just as it has maintained the security of data collected from existing meters. With smart meters, data recorded will be encrypted and transmitted to DP&L via a secure network that complies with the industry's standards for cybersecurity. DP&L's plan is to have encrypted point-to-point communication paths to each device from its primary application. This approach mitigates security risks by limiting the number of authorized communication endpoints of each field-deployed device. DP&L will safeguard customer information by incorporating industry best practices, hardened security methodologies and state-of-the-art protection technologies. Customers with smart meters will be able to access their own data securely through an online interface or other secure process. DP&L will not sell or trade customers' personal information to any third party, unless specifically authorized by the customer or by law. DP&L anticipates using industry standard protocols to share interval usage data with customer-authorized third parties. DP&L also plans to participate in the DWG outlined in the Commission's PowerForward Roadmap to ensure consistency and continued data privacy protections for customers.

DMP Security Project Three: Compliance Program

A Compliance Program for the DMP is critical to validate operational consistency, reliability, and the confidentiality, integrity and availability of DP&L's security operations. For example, NERC CIP regulatory programs enforce mandatory requirements for in-scope business operations that fall under NERC CIP compliance standards. As such, DP&L will implement a robust DMP Compliance Program to enforce federal, state and industry regulations or compliance requirements. The Compliance Program will have oversight and enforcement of activities that include:

1. Physical security risks and vulnerabilities related to the reliable operation of DP&L's bulk electric system, including transmission substations.
2. Sabotage incident investigations and regulatory reporting.
3. Identify and document the critical cyber assets associated with the critical assets that support the reliable operation of DP&L's bulk electric system.
4. Oversee minimum security management controls to protect DP&L's critical cyber assets according to DP&L's cybersecurity standards.
5. Manage DP&L's personnel with authorized cyber or unescorted physical access to DP&L's critical cyber assets, including contractors and service vendors, and ensure that DP&L personnel have an appropriate level of personnel risk assessment, training and security awareness.
6. Manage the identification and protection of DP&L's electronic security perimeters inside which all critical cyber assets reside, as well as all access points on the perimeter.

7. Maintain a physical security program for the protection of DP&L's critical cyber assets.
8. Manage the methods, processes, and procedures for securing DP&L's critical cyber assets, as well as the other (non-critical) cyber assets within DP&L's electronic security perimeters.
9. Ensure the identification, classification, response and reporting of cyber-security incidents related to DP&L's critical cyber assets.
10. Ensure that recovery plans are put in place for DP&L's critical cyber assets and verify the plans follow established business continuity and disaster recovery techniques and practices.

The performance of the Compliance Program will be monitored and reported on to senior leadership. This monitoring allows management to uncover trends in a timely manner and to address issues proactively. It also ensures a culture of compliance, and proactively addresses any problems should they arise.

DMP Security Project Four: Secure Digitalization

The DP&L DMP Security Model will use digitalization, automation, data analytics, and artificial intelligence to enhance and protect DP&L's investment, customer data, and those authorized to access it. Secure Digitalization will ensure the customer experience is cybersafe while providing enhancements to utility services. Automation within the cyberspace will provide faster transaction-based operations such as alert monitoring and event correlation, which will allow for quicker detections of security anomalies within the DMP. Data analytics provides the backbone of threat intelligence, offering improved

risk modeling and awareness of trends before they occur. Artificial intelligence allows security teams to leverage computer learning for security operations, business continuity, threat detection, and potential data exposures. When combined, these four digital processes act as a multiplier to the Security organization and its core mission of securing DP&L assets, processes and customer data.

Q. When does DP&L expect work on the Physical & Cyber Security Project to begin and to be completed?

A. DP&L expects to begin implementation of the Physical & Cyber Security Projects in the first year following the Commission's approval of the DMP and finish implementation over a period of ten years.

Q. What investments does DP&L anticipate making to implement the Physical & Cyber Security Projects?

A. DP&L plans to invest approximately $12 million in security enhancements over the life of the DMP project, categorized as $4.2 million in physical security enhancements, and $7.8 million in cybersecurity enhancements. These Physical and Cyber Security Projects capital investments are outlined in **Workpaper WP-6** "Physical Security Capital and O&M" summarizing project costs. A component of cybersecurity capital expenditures may be re-appropriated toward operational expenditures due to the proliferation of managed cybersecurity services and security service platforms maturing the market place, providing a lower overall cost to customers. In such a case, DP&L seeks permission from the Commission to treat those operational expenditures as capital.

Q. How were the estimates of capital and O&M expenditures on WP-6 prepared?

A. DP&L performed an assessment of the business requirements and necessary security measures required to adequately protect the data, assets and processes expected for implementation within the DMP. Workshops were held to review industry best practices, existing DP&L security architectures, and future-state technology to calculate estimated costs and services needed. Finally, a review of compliance-driven requirements was performed. The results of these discussions, reviews and assessments led to the creation of an itemize list of assets, platforms and services needed to support the security technologies as defined in WP-6.

III. CONCLUSION

Q. Please summarize your testimony.

A. A robust security program is crucial to the long-term sustainability of DP&L's power grid and a properly executed DMP. The details listed in this testimony outline significant physical security and cybersecurity upgrades to fully support a secure DMP environment.

Q. Does this conclude your direct testimony?

A. Yes.

Summary: Testimony Direct Testimony of Jeffrey K. Fuller electronically filed by Mr. Jeffrey S Sharkey on behalf of The Dayton Power and Light Company