BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

Petition of PPL Electric Utilities Corporation for Approval of Tariff Modifications and Waivers of Regulations Necessary to Implement its Distributed Energy Resources Management Plan	: : : : :	Docket No. P-2019-3010128

DIRECT TESTIMONY OF AARON BAYLES

PPL Electric Statement No. 5

December 11, 2019

Q. PLEASE STATE YOUR NAME AND BUSINESS ADDRESS.

A. My name is Aaron Bayles, and my business address is 350 Sentry Parkway Bldg. 670, Suite 201 Blue Bell, PA 19422.

Q. BY WHOM ARE YOU EMPLOYED AND IN WHAT CAPACITY?

A. I am employed by Revolutionary Security LLC ("Revolutionary Security") as a Principal Cybersecurity Consultant and OT Testing & Assessments Service Lead.

Q. WOULD YOU PLEASE DESCRIBE REVOLUTIONARY SECURITY LLC?

A. Revolutionary Security is an experienced team of cybersecurity professionals whose mission is to provide its clients with the knowledge and expertise to defend their enterprises against cyber threats. The business's cybersecurity consulting and advisory services focus on helping its clients evolve their capabilities across the entire spectrum of people, process, and technology.

Revolutionary Security's services span both IT and industrial control system security projects across sectors including electric utilities, oil & gas, manufacturing, technology & communication, financial, transportation, and health & life sciences. The business is currently delivering cybersecurity services to utilities that serve over 110,000,000 customers.

Q. WHAT ARE YOUR DUTIES AS PRINCIPAL CYBERSECURITY CONSULTANT?

A. I perform cybersecurity related projects and tasks for the clients of Revolutionary Security. These projects are focused in the business's Operational Technology (OT) Security practice.

Q. WHAT IS YOUR EDUCATIONAL BACKGROUND?

A. I received a Bachelor of Science degree in Computer Science from Sam Houston State University in December 2001. I have also taken post-graduate classes in Embedded Linux Programming. My certifications include Certified Information Systems Security Professional (CISSP #81610).

Q. PLEASE DESCRIBE YOUR PROFESSIONAL EXPERIENCE.

A. I have over 23 years' experience within the utility, oil & gas, financial, government, energy, and education industries focused on information and cybersecurity in both Information Technology (IT) and Operational Technology (OT). Recently, I have been the lead on a utility cybersecurity rate case filing and led Incident Response activities for oil & gas clients. I am the technical lead on numerous Industrial Control Systems (ICS) projects for Revolutionary Security's clients.

I have helped clients in multi-year strategies to design and implement architectures to align against regulatory and industry best practices. I also regularly speak at security conferences around the United States.

Q. HAVE YOU PREVIOUSLY TESTIFIED AS A WITNESS BEFORE THE PENNSYLVANIA PUBLIC UTILITY COMMISSION ("COMMISSION")?

A. No.

Q. HAVE YOU BEEN RETAINED BY PPL ELECTRIC UTILITIES CORPORATION ("PPL ELECTRIC" OR THE "COMPANY") TO TESTIFY ON BEHALF OF THE COMPANY IN SUPPORT OF THE ABOVE-CAPTIONED PETITION?

A. Yes.

Q. WOULD YOU PLEASE DESCRIBE THE SUBJECT MATTER OF YOUR TESTIMONY?

A. My testimony will address cybersecurity issues related to the Company's proposal and explain the steps PPL Electric will take to protect its customers' data from unauthorized public disclosure under its DER Management Plan.

Q. ARE YOU SPONSORING ANY EXHIBITS WITH YOUR TESTIMONY?

A. No.

A. CYBERSECURITY PRACTICES AND PROTOCOLS

Q. WOULD YOU PLEASE EXPLAIN YOUR UNDERSTANDING OF THE COMPANY'S DER MANAGEMENT PLAN, WITH PARTICULAR FOCUS ON THE COMMUNICATIONS DEVICES INVOLVED?

A. Yes. My understanding is that under the Company's DER Management Plan, PPL Electric would require new Distributed Energy Resources ("DERs") interconnected with the Company's distribution system to have DER management devices installed and connected to the local communication interface of the DER system, so that PPL Electric can monitor and manage the DERs and take advantage of the DERs' grid support functions. As explained by PPL Electric witness Sal Salet (PPL Electric Statement No. 1), the Company envisions two types of DER management devices being used: (1) mesh network radios; or (2) cellular modems. Descriptions of those devices are set forth in Mr. Salet's direct testimony. PPL Electric also is working with an outside vendor to develop a compact device to integrate with the DER's smart inverter and use the RF Mesh network for communication. Revolutionary Security will perform security testing on this device prior to use by PPL Electric's customers.

Q. ARE YOU FAMILIAR WITH THE COMPANY'S RADIO FREQUENCY ("RF") MESH NETWORK THAT WOULD BE USED UNDER THE FIRST OPTION?

A. Yes. The RF Mesh environment consists of radios that transmit and receive on the 900 MHz Industrial, Scientific, and Medical (ISM) bands. This RF Mesh system is a network that can be used to connect the Company's distribution system to the local communication interface of the DER's smart inverter. Network communication between the distribution system and the DER is encrypted across the RF Mesh environment and decrypted at the 900 MHz radio connecting via a physical serial interface to the DER.

In July and September of 2019, I led members of Revolutionary Security's Operational Technology Security team in performing security testing that encompassed

the 900 MHz radios, the RF Mesh environment, the DER and smart inverter, and the cellular modems used as another communication medium between the Distribution Energy Resource Management System ("DERMS"), the DERMS software, and the DER. This security testing involved discovery workshops, vulnerability assessment, and penetration testing simulating different adversarial approaches. These approaches were based on the amount of knowledge and inside information (credentials, manuals, detailed system documentation) available to the testing team. The testing simulated attack by an adversary with zero knowledge of the environment and an adversary with insider knowledge about the applications and infrastructure.

Q. WOULD YOU PLEASE EXPLAIN THE CYBERSECURITY PRACTICES AND PROTOCOLS THAT THE COMPANY HAS DEVELOPED TO HELP PROTECT AGAINST THE UNAUTHORIZED DISCLOSURE OF INFORMATION TRANSMITTED ON THE RF MESH NETWORK?

A. The RF Mesh connection between the DER and the Company's distribution system is protected by Advanced Encryption Standard (AES) encryption with unique strong credentials. Encryption keys are unique to each radio, which prevents interception or unauthorized disclosure of the information that is carried across the RF Mesh network. Access to the RF Mesh network is restricted by multiple access control devices that prevent unauthorized usage.

Revolutionary Security's team interviewed the PPL Electric personnel responsible for the DER communications, reviewed their documentation and sample data, and

validated that only solar generation data is sent by the DER and it does not include any customer identifiable information.

The cybersecurity best practices of network segmentation[1], defense-in-depth[2], and least privilege[3] are reflected in the RF Mesh network design and interconnections. The RF Mesh network is separated from other PPL Electric networks by using firewalls and other access control mechanisms, such as multi-factor authentication ("MFA") that requires the user to enter an additional code that changes every 30 seconds to login, which prevent unauthorized persons or applications from accessing the RF Mesh. Within the RF Mesh, the encryption uses the AES algorithm with 256-bit length keys to prevent disclosure or modification of any information that crosses the network. The communication protocols used across the RF Mesh are specialized for OT applications and not general-purpose Information Technology (IT). This reduces the attack surface presented by the RF Mesh to an attacker.

Q. FROM YOUR PERSPECTIVE, DOES THE USE OF THE COMPANY'S RF MESH SYSTEM UNDER PPL ELECTRIC'S PROPOSAL RAISE ANY CYBERSECURITY CONCERNS?

A. No. The protections built into the Company's RF Mesh network are explicitly designed to prevent unauthorized use and access. The RF Mesh network is monitored by

[1] Network segmentation is the practice of separating systems with different function, capability, or security characteristics by restricting communication between different networks. *See* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf - Page 19.

[2] Defense-in-depth uses layers of differing security controls to increase the capability of stopping or reducing the impact of attackers. *See* https://csrc.nist.gov/glossary/term/defense_in_depth.

[3] Least privilege only grants the minimum amount of access necessary to perform a task, and not excessive or unnecessary permissions. *See* https://csrc.nist.gov/glossary/term/least-privilege.

technologies that will alert on attempts to bypass security protections. It is part of the Company's policies and procedures to regularly scan and test that the security protections are operational and apply updates to maintain the cybersecurity posture. This testing and scanning will continue to occur if the RF Mesh is used as the DER communication method.

In addition, the DER with the smart inverter was a focus of Revolutionary Security's cybersecurity testing due to the connection to the customer's Wi-Fi network. The security controls provided by a customer's Wi-Fi network vary greatly depending on the way they are configured. This is a communication method to the smart inverter and DER that is outside the control of the Company. Any DER with a smart inverter has the same risk of compromise from the customer's Wi-Fi.

Q. AS FOR THE SECOND OPTION USING CELLULAR MODEMS, ARE YOU FAMILIAR WITH THE COMPANY'S CURRENT USE OF SUCH COMMUNICATION DEVICES ON ITS DISTRIBUTION SYSTEM?

A. Yes. The Company uses cellular modems that utilize a commercial network (Verizon or AT&T) to communicate from the distribution endpoint to the Company's distribution systems. The physical Ethernet interface provided by the cellular modem can be configured to communicate with the smart inverter of the DER. This allows the Company's distribution systems to send and receive information to and from the DER.

During the cybersecurity testing in July and September of 2019, Revolutionary Security's team also performed directed testing against the cellular modem. This testing

included the physical Ethernet interfaces, physical serial interface, and the software built-into the cellular modem itself.

Q. WOULD YOU PLEASE EXPLAIN THE CYBERSECURITY PRACTICES AND PROTOCOLS THAT THE COMPANY HAS DEVELOPED TO HELP PROTECT AGAINST THE UNAUTHORIZED DISCLOSURE OF INFORMATION TRANSMITTED THROUGH CELLULAR DEVICES?

A. Similar to the RF Mesh network design and interconnections, the cybersecurity best practices of network segregation, defense-in-depth, and least privilege are reflected in the cellular modem implementation. Access to the cellular network is separated from other PPL Electric networks by using firewalls and other access control mechanisms that prevent use by unauthorized persons or applications. Distribution system information transmitted across the cellular network is protected by encryption and isolation provided by the cellular network and is used to prevent disclosure or modification of any information that crosses the network. The communication protocols used across the cellular network are specialized for OT applications and not general-purpose Information Technology (IT).

Q. FROM YOUR PERSPECTIVE, DOES THE USE OF CELLULAR DEVICES UNDER PPL ELECTRIC'S PROPOSAL RAISE ANY CYBERSECURITY CONCERNS?

A. No, the use of cellular modems does not raise any cybersecurity concerns. Similar to the RF Mesh network, the protections built into the cellular modem and cellular network are

explicitly designed to prevent unauthorized use and access. Access to the cellular network from the Company's network is monitored by technologies that will alert on attempts to bypass security protections. It is part of the Company's policies and procedures to regularly scan and test that the security protections are operational and apply updates to maintain the cybersecurity posture. This scanning and testing will continue if the cellular network is used to communicate information for the DERs.

Q. UNDER EITHER THE RF MESH NETWORK OPTION OR THE CELLULAR MODEM OPTION, CAN YOU EXPLAIN WHAT CUSTOMER DATA WILL BE TRANSMITTED FROM THE DERS TO PPL ELECTRIC?

A. Yes. Regardless of the communication option, the data transmitted from the DER to the Company consists of a unique identifier tied to the DER and smart inverter and solar generation production values at the time of polling. The solar generation production values will include the following information: meter or transformer identifier, date & time, type of positive or negative kilowatt hour ("kWh"), and the amount of kWh generated.

Q. HOW WILL THE COMPANY PROTECT THAT CUSTOMER DATA AFTER IT HAS BEEN TRANSMITTED FROM THE DERS?

A. The Company considers the privacy of customers' information as a high priority. It has implemented systems that isolate and segregate customer information from environments that do not require that information. Additional authentication requirements and secured network transport is required to access systems that process and store customer

information transmitted from the DERs. These systems are regularly scanned for cybersecurity vulnerabilities and configurations which may put the system integrity at risk. Issues discovered from these scans and tests are remediated commensurate with the criticality of the system. Information transmitted from DERs will be protected in the same manner from unauthorized use or disclosure. The protection mechanisms and regular scan and test requirements are aligned with the industry best practices for cybersecurity.

Q. DOES THE COMPANY CONTINUALLY ASSESS ITS SYSTEMS AND PRACTICES FOR POTENTIAL SECURITY GAPS AND ISSUES?

A. Yes. The Company regularly performs automated vulnerability assessments scans against their infrastructure that look for outdated system and application updates, misconfigurations of services, and the use of default or vendor provided credentials. The scans are part of a cybersecurity program that is equivalent or better than utility industry standards. The Company also utilizes third-party companies to perform independent testing of their systems to ensure that vulnerabilities are not overlooked and that their cybersecurity controls work as intended. The Company's cybersecurity program including vulnerability scans and third-party testing will continue after the Petition is approved.

Q. DOES THIS CONCLUDE YOUR DIRECT TESTIMONY AT THIS TIME?

A. Yes, although I reserve the right to supplement my direct testimony.

VERIFICATION

I, AARON BAYLES, being a Principal Cybersecurity Consultant and OT Testing & Assessments Service Lead at Revolutionary Security LLC, hereby state that the facts above set forth are true and correct to the best of my knowledge, information and belief and that I expect PPL Electric Utilities Corporation to be able to prove the same at a hearing held in this matter. I understand that the statements herein are made subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

Date: 12/10/19

Aaron Bayles