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

REBUTTAL TESTIMONY OF AARON BAYLES

PPL Electric Statement No. 5-R

March 4, 2020

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. HAVE YOU PREVIOUSLY SUBMITTED IN DIRECT TESTIMONY IN THIS PROCEEDING?

A. Yes. My direct testimony is set forth in PPL Electric Statement No. 5.

Q. WHAT IS THE PURPOSE OF YOUR REBUTTAL TESTIMONY?

A. I will respond to allegations made in: NRDC Statement No. 1, the Direct Testimony of Harry Warren submitted on behalf of the Natural Resources Defense Council ("NRDC"); OCA Statement No. 1, the Direct Testimony of Ron Nelson submitted on behalf of the Office of Consumer Advocate ("OCA"); SEF Statement No. 1 (Non-Proprietary Version), the Direct Testimony of John Costlow submitted on behalf of the Sustainable Energy Fund ("SEF"). My rebuttal testimony specifically focuses on the cybersecurity issues raised by customers and third-party distributed energy resource ("DER") aggregators providing smart inverter data to the Company, rather than PPL Electric being able to receive the data directly from the smart inverters through the DER management devices.

I. CYBERSECURITY ISSUES RAISED BY CUSTOMERS AND THIRD-PARTY DER AGGREGATORS COMMUNICATING WITH AND MANAGING SMART INVERTERS INSTEAD OF PPL ELECTRIC

Q. QUESTIONS HAVE BEEN RAISED ABOUT THE IMPACT, IF ANY, OF THE COMPANY'S PROPOSAL ON CUSTOMERS AND THIRD-PARTY DER AGGREGATORS BEING ABLE TO COMMUNICATE WITH AND MANAGE THE SMART INVERTERS. (NRDC ST. NO. 1, PP. 8-9; OCA ST. NO. 1, PP. 18-28, 42-44; SEF ST. NO. 1 (NON-PROPRIETARY), PP. 4, 14-15.) HOW DO CUSTOMERS AND THIRD-PARTY DER AGGREGATORS COMMUNICATE WITH AND MANAGE SMART INVERTERS?

A. The smart inverter that Revolutionary Security tested relies upon the customer's wireless (Wi-Fi) or Ethernet network to provide an Internet-based connection to the smart inverter manufacturer's or third-party DER aggregator's online portal.

Q. ARE THE CUSTOMERS' NETWORKS GENERALLY CONSIDERED TO BE SECURE FROM A CYBERSECURITY PERSPECTIVE?

A. No. There is no cybersecurity standard that is generally applied to the configuration of personally owned and operated networks. Although Internet routers and related devices used to access the Internet have capabilities that provide protections and remediations against attackers, it is challenging for customers to configure and maintain their equipment to defend against attackers. There are ways that attackers bypass these

defenses utilizing technical and inter-personal techniques, such as "drive-by malware"[1] and social engineering using phishing and pretexts[2].

During the testing, referenced on pages 4-5 of my direct testimony (PPL Electric Statement No. 5), Revolutionary Security simulated attacks from varying levels of knowledge and access. This included testing from an "assume breach" model,[3] where it is assumed that the attacker has compromised cybersecurity protections and has full network access to the target system, in this case the smart inverter. Based on the assume breach model, via a targeted attack or by a simple misconfiguration, it is difficult to ensure that any Internet-based communication to manufacturer or third-party DER online portal has not been compromised. Once compromised, the attacker can change the settings for grid support functions or other smart inverter parameters and can compromise the accuracy of the data transmitted by the smart inverter.

Q. OCA WITNESS NELSON ALSO ALLEGES THAT "IT IS UNCLEAR WHETHER THE COMPANY HAS CONSIDERED ALTERNATIVE APPROACHES FOR GETTING INFORMATION THAT MAY BE USED TO TROUBLESHOOT LOAD MASKING ISSUES" AND THAT "NUMEROUS

---

[1] "Drive-by malware" is when the user clicks on a link to malicious software provided from a search engine result or via other redirection of what appears to be a valid result. https://arstechnica.com/information-technology/2019/06/new-ransomware-infections-are-the-worst-drive-by-attacks-in-recent-memory/

[2] Social engineering attacks use subterfuge and misdirection to coerce a user into performing an action to provide potentially sensitive access or information to an attacker. https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[3] "Microsoft operates under an "Assume Breach" posture. This means that despite all the protections in place, we assume systems will fail or people will make errors, and an adversary may penetrate our infrastructure and services. This posture places us in an "always ready" position to rapidly detect a compromise and take appropriate actions." https://download.microsoft.com/download/4/6/8/4680DFC2-7D56-460F-AD41-612F1A131A26/Microsoft_Cyber_Defense_Operations_Center_strategy_brief_EN_US.pdf

STATES HAVE REQUIRED THAT CUSTOMERS PROVIDE INVERTER DATA FROM DERS." (OCA ST. NO. 1, PP. 16-17.) DO THESE "ALTERNATIVE APPROACHES" INVOLVING CUSTOMERS OR THIRD-PARTY DER AGGREGATORS PROVIDING INVERTER DATA TO ELECTRIC UTILITIES PRESENT CYBERSECURITY CONCERNS?

A. They absolutely present cybersecurity concerns. Although there are methods available to provide a secure communications path between PPL Electric and data providers, such as customers and third-party DER aggregators, when the fidelity of the connection from the smart inverter to those data providers cannot be attested, then the data itself may not be correct, accurate, or protected from disclosure.

Q. DOES THE COMPANY'S DER MANAGEMENT PROPOSAL RAISE ANY SIMILAR CYBERSECURITY CONCERNS?

A. No. PPL Electric's choice to interface with the smart inverter via serial communication eliminates the risk posed by the customer's Wi-Fi and Ethernet networks on the smart inverter. The SunSpec Modbus[4] protocol used over the serial connector is limited in visibility to the smart inverter settings and information to which it has access. Being a limited visibility interface, the serial interface has a smaller attack surface than the Wi-Fi and Ethernet interfaces. The testing performed by Revolutionary Security, which is described on pages 4-5 of my direct testimony (PPL Electric Statement No. 5), included techniques to determine if an attacker-compromised smart inverter would be able to

[4] "SunSpec Modbus is an open standard, referenced in IEEE 1547-2018, that enables interoperability amongst DER system components."
https://sunspec.org/sunspec-modbus/

connect to any other PPL Electric network. To simulate a bypass of the smart inverter, Revolutionary Security connected testing equipment directly to a Radio Frequency ("RF") Mesh radio and to a cellular modem to try to use those communication channels to communicate with PPL Electric's protected networks. This approach was chosen because it confirms the cybersecurity of PPL Electric's networks and software including DERMS even if the customer's smart inverter is fully compromised. Due to the defense-in-depth techniques described on pages 5-6 and on page 8 of my direct testimony (PPL Electric Statement No. 5), Revolutionary Security was unable to connect to any other PPL Electric networks. These testing results demonstrate that the design of PPL Electric's solution protects both customer information and other PPL Electric networks. Simply put, the Company's DER Management proposal is much better protected against cybersecurity threats than alternatives approaches where customers and/or third-party DER aggregators communicate with and obtain data from the smart inverters.

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

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