STATE OF NEW JERSEY
BOARD OF PUBLIC UTILITIES

In the Matter of the Petition of Public Service Electric and Gas Company for Approval of an Increase in Electric and Gas Rates and for Changes in the Tariffs for Electric and Gas Service, B.P.U.N.J. No. 16 Electric and B.P.U.N.J. No. 16 Gas, and for Changes in Depreciation Rates, Pursuant to N.J.S.A. 48:2-18, N.J.S.A. 48:2-21 and N.J.S.A. 48:2-21.1, and for Other Appropriate Relief

BPU Docket Nos. _____

DIRECT TESTIMONY
OF
AARON T. FORD

VICE PRESIDENT - CORPORATE SECURITY AND CLAIMS
PSEG SERVICES CORPORATION

January 12, 2018
P-11

PUBLIC SERVICE ELECTRIC AND GAS COMPANY
DIRECT TESTIMONY
OF
AARON T. FORD
VICE PRESIDENT - CORPORATE SECURITY AND CLAIMS

Q. Please state your name and business address.

A. My name is Aaron T. Ford. My business address is 80 Park Plaza, Newark, New Jersey.

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

A. I am employed by PSEG Services Corporation as the Vice President of Corporate Security and Claims ("CSAC"). I am the senior most leader for the Company's security and claims departments. Prior to joining PSEG Services Corporation, I worked for the Federal Bureau of Investigation for 30 years before retiring in 2015. My last position with the FBI was the head of its Newark, New Jersey division. My professional credentials are more fully set forth in Schedule ATF-1.

Q. What is the purpose of your testimony?

A. In this case, I am testifying on behalf of Public Service Electric and Gas Company ("PSE&G" or "the Company"). The purpose of my testimony is to summarize the Company's cybersecurity program.

Q. What is cybersecurity?

A. Cybersecurity is the process by which the Company protects the confidentiality, integrity, and accessibility of its computing platforms and communication networks as well as the sensitive data stored and transmitted across those systems, such as customers' and

employees' personally identifiable information ("PII"). As is now well known through recent incidents like the cyber attacks against the Ukraine electric system, the WannaCry ransomware event, and the Equifax data breach, the private sector -- and the energy sector in particular -- is a frequent target of cyber actors who seek to penetrate companies' computer networks for a variety of malevolent reasons, including financial gain, to serve state-sponsored objectives, vanity, or humiliating the entities or individuals who are victimized by the cyber attack.

Q. Why is cybersecurity so important?

A. Cybersecurity is important to a company like PSE&G for two principal reasons. First, preventing a cyber attack on the critical infrastructure we own and operate is a matter of national security and imperative to a fully functioning society. PSE&G is a public utility serving approximately 2.2 million electric customers and 1.8 million gas customers across New Jersey, including countless hospitals, police and fire departments, government facilities, and schools. The integrity and accessibility of the control systems that operate our electric and gas distribution systems is of vital importance. Second, the confidentiality of our customers' and employees' PII is of the utmost significance, and it would be compromised if a hacker accessed this sensitive information through a cyber attack. The unauthorized access to PII on PSE&G's computer system may lead to financial harm, adverse credit ratings, and embarrassment for our customers and employees. Over time, cyber threats have become more sophisticated and common. Cyber attacks against companies -- including reputable companies with significant resources -- are becoming a common occurrence. All of this means that cybersecurity is more important now than ever before.

Q. How is the Company responding to cybersecurity risks?

A. As an initial matter, PSE&G's parent company has made cybersecurity an integral part of its corporate governance. For example, we: made cybersecurity a Scorecard metric; internally publish cybersecurity guidance, practices, expectations, and incident response plans; draft cybersecurity awareness campaigns that the Company disseminates to its employees electronically and via bulletin board postings; require all employees and contractors with computing system access to undergo annual and new-hire cybersecurity training; conduct additional cybersecurity training for employees and contractors with privileged user access (i.e., Information Technology ("IT") employees and contractors, employees and contractors with access to industrial control systems, or administrators of customer information systems containing PII); conduct phishing exercises to help educate and test the effectiveness of our employees in recognizing common phishing tactics to avoid such an attack; formed a "cybersecurity council" consisting of top-level executives that meets monthly to discuss emerging cybersecurity issues; and are focused on reducing -- if not eliminating -- the customer PII we store on our computer networks.

Q. Is there anything else the Company is doing to mitigate cybersecurity risks?

A. Yes. We employ technical safeguards to help reduce the chance of a cyber attack or mitigate the impact if one were to occur. These include measures to protect the network perimeter and internal IT platforms such as: internal and external firewalls, network intrusion detection and prevention, penetration testing, vulnerability assessments, content filtering and analysis, strong access authentication requirements, anti-malware, least privileges (i.e.,

granting employees the least amount of network access necessary for them to adequately perform their jobs), log reviews, access controls, and access entitlement reviews.

Q. What else is the Company doing to enhance cybersecurity?

A. PSE&G is also focused on maintaining what is referred to as "situational awareness." By that I mean keeping up to date on various cybersecurity materials, alerts, and notices that external entities disseminate or offer. This includes reviewing bulletins and advisories from our vendors; participating in key industry security efforts such as those the Edison Electric Institute and American Gas Association lead; analyzing government and information sharing analysis center alerts and advisories, such as the Homeland Security Information Network, the Electricity and Downstream Natural Gas Information Sharing and Analysis Centers, the FBI, the New Jersey Cybersecurity and Communications Integration Cell, and information provided by the Federal Trade Commission; receiving updates, briefings, and feedback on our cybersecurity program from law enforcement agencies such as the FBI and the U.S. Department of Homeland Security, as well as the U.S. Department of Energy; and attending the BPU's annual cybersecurity summit.

Q. What steps has the Company taken to prepare to respond to a cyber attack in the event one was to occur?

A. The Company maintains cybersecurity incident and data breach response plans that it would activate in the event of a cyber incident. The cybersecurity incident response plan is a technical manual that addresses the life cycle of a cyber incident, *i.e.,* detection, response, and recovery. It contains defined methodology and changing team composition depending on four event severity levels. The data breach response plan addresses the life cycle of a data

breach, such as the unauthorized access of customer or employee PII. It also lists defined roles and responsibilities, as well as templates for incident response and communications, such as notification letters to governmental agencies and individuals whose PII were compromised.

Q. What does the Company do to test the effectiveness of these plans?

A. The Company tests or exercises these plans at least annually. This may include participation in external exercises organized by state or federal agencies -- like the BPU's May 2017 Black Sky tabletop exercise -- or industry groups -- like the electric industry's bi-annual Grid Ex exercises. It may also include internal tabletop exercises. For example, I am responsible for overseeing the Company's Executive Crisis Management Team ("ECMT"). The ECMT is comprised of Company executives and officers from across PSEG who would be called upon to take action on behalf of the Company in the event of a crisis situation, such as a significant cyber attack. The last two ECMT tabletop exercises -- including the most recent one in June 2017 -- focused on a cyber incident. The Company incorporates lessons learned into its cyber incident response and data breach plans after these events and exercises.

Q. Do these cybersecurity measures you have described serve any purpose other than maintaining good cyber hygiene?

A. Yes. As a regulated public utility owning and operating critical infrastructure, we are subject to a myriad of regulations and requirements related to cybersecurity. The cybersecurity measures to which I have testified above help us satisfy our regulatory obligations. These obligations arise from various sources, such as the BPU's March 18, 2016

Cybersecurity Order (Docket No. AO16030196) and the North American Electric Reliability Council's Critical Infrastructure Protection standards.

Q. Does this conclude your testimony?

A. Yes, it does.

CREDENTIALS
OF
AARON T. FORD
VICE PRESIDENT CORPORATE SECURITY AND CLAIMS

My name is Aaron T. Ford and I am employed by Public Service Enterprise Group Services Corporation (PSEG or the Company) as the Vice President – Corporate Security and Claims (previously known as "Business Assurance and Resilience"). In this role, I am the designated, executive-level personnel with authority over the Company's cybersecurity program pursuant to the Board of Public Utilities cybersecurity Order dated March 18, 2016 in BPU Docket No. A016030196. I also have primary management and oversight responsibility for the Company's corporate security and claims functions, including business continuity and crisis management planning.

EDUCATIONAL BACKGROUND

I have a Bachelor of Science degree in Criminology from Tennessee State University and a Juris Doctor degree from Rutgers School of Law.

WORK EXPERIENCE

I have worked for PSEG Services Corporation for over two and a half years, as well as 30 years as a special agent with the Federal Bureau of Investigation in various supervisory and executive positions in numerous locations within the United States. As the Special Agent in Charge, I had oversight of all investigative

and administrative matters for most of New Jersey, including five satellite offices within the Newark division territory. I worked closely with other law enforcement agencies in responding to priority threats, oversaw budgets, and established strategic planning and crisis preparedness for the federal government during Super Bowl XLVIII in New Jersey. Previously, I served as the Special Agent in Charge, Memphis division, and served several stints at the FBI headquarters, where I oversaw field office and headquarters compliance inspections, and led shooting incident review teams.

I joined PSEG in February of 2015 as Director of Homeland Security, and assumed the role of Vice President – Corporate Security and Claims in November of 2015 (then referred to as "Business Assurance and Resilience"). As Vice President – Corporate Security and Claims, I am responsible for developing and effectuating PSEG's enterprise-wide strategies for homeland security; asset protection; business continuity and crisis management; "OPSEC" or Information Security, including electronics, forensics, and litigation support; physical security programs; security regulatory compliance; intelligence acquisition and analysis; law enforcement and intel agency liaison at the most senior levels; and security policy-making. In addition, I have responsibility for PSEG's uninsured claims program.

I am a member of the Domestic Security Alliance Council and serve as the Vice Chair of the Infrastructure Advisory Committee for New Jersey. I am also a

member of the Public Sector Advisory Group for the region. I currently hold memberships with the American Society for Industrial Security, Global Security Executives and the Global Security Executives Roundtable groups.