Company Exhibit_____

BEFORE THE
PUBLIC UTILITIES COMMISSION OF OHIO

In the Matter of the Filing by Ohio Edison Company, The Cleveland Electric Illuminating Company, and The Toledo Edison Company for a Distribution Platform Modernization Plan	))))))	Case No. 17-2436-EL-UNC

DIRECT TESTIMONY OF

BRANDON W. BOLON

ON BEHALF OF

OHIO EDISON COMPANY
THE CLEVELAND ELECTRIC ILLUMINATING COMPANY
THE TOLEDO EDISON COMPANY

December 1, 2017

INTRODUCTION

Q. PLEASE STATE YOUR NAME, POSITION, AND BUSINESS ADDRESS.

A. My name is Brandon W. Bolon. I am employed by FirstEnergy Service Company as Manager, Corporate Cyber Security. My business address is 76 S. Main Street, Akron, Ohio 44308.

Q. PLEASE STATE YOUR EDUCATION AND WORK HISTORY.

A. I graduated from Ohio University in 2000 with a double major in management and management information systems, along with a minor in interpersonal communications. I obtained my Certified Information Systems Security Professional (CISSP) certification in 2006. I have worked for FirstEnergy Service Company or subsidiaries of FirstEnergy Corp. ("FirstEnergy") for 17 years and have held various management positions within Information Technology ("IT"). Early in my career, I helped lead the implementation of FirstEnergy's cyber security strategy, which included establishing the cyber security organization and program. In my current role, my responsibilities include managing the enterprise cyber security program and governance, incident response, training and awareness, vulnerability management, and the security technology hardware and software. In this role, I provide support to all subsidiaries of FirstEnergy, including Ohio Edison Company, The Cleveland Electric Illuminating Company, and The Toledo Edison Company (collectively, the "Companies").

CYBER SECURITY

Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY?

A. The purpose of my testimony is to describe the cyber security program applicable to the Companies' proposed Distribution Platform Modernization ("DPM") Plan.

Q. PLEASE PROVIDE AN OVERVIEW OF FIRSTENERGY'S CYBER SECURITY PROGRAM.

FirstEnergy has an enterprise cyber security program in place that incorporates best practices to prevent, detect, respond and recover from cyber threats. FirstEnergy has implemented a defense-in-depth strategy for perimeter and internal defenses including routers, firewalls, demilitarized zone (DMZ), intrusion prevention and detection, second factor authentication, logging and monitoring, and malicious software prevention. This program is built on strong, well-established policies, standards and procedures covering all aspects of FirstEnergy's operations. Aspects of FirstEnergy's cyber security program include, but are not limited to: device baselines for hardening; acceptable network usage; background checks on employees/contractors and vendors; limiting access based on least privilege; elevated account separation; secure password vaulting for shared, service and built-in accounts; providing physical protection and security to the hardware; using strong authentication to verify the identity of those users that access the network; and separation of critical network segments.

Q. **IS FIRSTENERGY'S CYBER SECURITY PROGRAM REVIEWED AND/OR TESTED BY A THIRD-PARTY?**

A. Yes. External and internal vulnerability and penetration tests are conducted by a third-party vendor every one to two years. The vendor is selected through an RFP process. In evaluating proposals, FirstEnergy performs a detailed review of the vendor's qualifications, ability to meet FirstEnergy's requirements, and the qualifications of the personnel that would conduct the assessment. Once selected, the vendor conducts its assessment. The results of the assessment are analyzed by FirstEnergy. As part of FirstEnergy's vulnerability

management process, any findings identified by the vendor are assigned a risk rating and remedial actions are taken as appropriate.

Q. HOW OFTEN IS FIRSTENERGY'S CYBER SECURITY INCIDENT RESPONSE PLAN TESTED?

A. The incident response plan is practiced several times a year through internal and external exercises.

Q. PLEASE DESCRIBE FIRSTENERGY'S CYBER SECURITY EDUCATION AND AWARENESS PROGRAMS.

A. FirstEnergy requires all employees and contractors that have access to FirstEnergy systems to annually take cyber security awareness training (CSAT). Those who have FirstEnergy email addresses are also required to take anti-phishing training. Elevated users are required to take elevated access training to understand their increased responsibility with the access that they have. Personnel that have access to Critical Infrastructure Protection (CIP) are required to also take annual CIP training.

Q. DOES FIRSTENERGY HAVE PROCESSES FOR IDENTIFYING POTENTIAL CYBER SECURITY RISKS?

Yes. FirstEnergy has in place an Application Development Methodology (ADM) that is followed for new systems. In addition, there is an Application Design Review (ADR) that is followed for any new technology (hardware/software) or major upgrade. The Cyber Security team, as well as other areas within IT, review the proposal to ensure it follows standards and policies before approving. This process also provides visibility for my team to ensure vulnerability scans and cyber security reviews are performed on new technology.

In addition, FirstEnergy has a vulnerability management program in place. This program covers the receipt of notifications of patches and other security vulnerabilities from subscription services, various government and third-party information sharing sources, and any findings from internal and external scans and results from third party testing. Any information that is received from external sources is reviewed and confirmed that it applies to FirstEnergy. Once confirmed, the information is assigned a risk rating and appropriate remedial actions acre taken to mitigate the identified risks.

Q. WHAT ASPECTS OF THE PROPOSED DPM PLAN WOULD BE SUBJECT TO FIRSTENERGY'S CYBER SECURITY PROGRAM?

A. In general, the DPM Plan will follow FirstEnergy's defined processes to review, identify, and assess any perceived security risks. The specific categories of work in the DPM Plan that would be subject to this review would include the data acquisition systems – SCADA and ADMS – which are described in the direct testimonies of witnesses Vallo and Rouse, respectively. The scope of the review would include, but would not be limited to, the design considerations of the network connectivity, along with the configuration of any hardware and software that would be implemented.

Q. WHAT IS THE PROCESS FOR ADDRESSING ANY CYBER SECURITY RISKS ASSOCIATED WITH THE DPM PLAN?

A. If there are any security risks identified, they will be reviewed in detail under FirstEnergy's cyber security program. Appropriate mitigation plans will be identified, reviewed, approved, tested and put in place prior to the projects moving to production. Examples of mitigation may include a configuration setting, patch, network segmentation utilizing access control list technology, or other controls to provide acceptable protection.

Q. PLEASE PROVIDE AN EXAMPLE OF A CYBER SECURITY RISK RELATED TO THE DPM PLAN AND HOW THE COMPANIES WOULD MANAGE IT.

A. One area of risk associated with the DPM Plan is the network connectivity and the exposed networks outside of FirstEnergy needed to facilitate communications with the SCADA devices. These network communications projects would be designed and reviewed by FirstEnergy's Cyber Security team to ensure the appropriate controls are in place so that only authorized users, devices, and data are permitted on the network and appropriate monitoring, detection, and response processes are in place. As discussed in the direct testimony of Companies' witness Vallo, FirstEnergy has recently invested in a 700 MHz block spectrum radio frequency bandwidth, which will help to minimize exposure of communication outside of the FirstEnergy network. While this investment is not included in the DPM Plan, it is a constructive example of the type of measure that the Companies will evaluate and pursue, if necessary, to mitigate cyber security risks associated with the DPM Plan.

Q. PLEASE SUMMARIZE YOUR CONCLUSIONS.

A. FirstEnergy has a robust cyber security program and a strong Cyber Security team in place to monitor, assess, and protect against potential cyber security risks associated with the DPM Plan.

Q. DOES THIS CONCLUDE YOUR TESTIMONY?

A. Yes; however, I reserve the right to supplement my testimony.

Summary: Testimony of Brandon W. Bolon electronically filed by Mr. James F Lang on behalf of Ohio Edison Company and The Cleveland Electric Illuminating Company and The Toledo Edison Company