**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF COLORADO**

*** * * * ***

RE: IN THE MATTER OF THE APPLICATION OF PUBLIC SERVICE COMPANY OF COLORADO FOR AN ORDER GRANTING A CERTIFICATE OF PUBLIC CONVENIENCE AND NECESSITY FOR DISTRIBUTION GRID ENHANCEMENTS, INCLUDING ADVANCED METERING AND INTEGRATED VOLT-VAR OPTIMIZATION INFRASTRUCTURE	**))))))))))**	**PROCEEDING NO. 16A-____E**

DIRECT TESTIMONY AND ATTACHMENTS OF DAVID C. HARKNESS

ON

BEHALF OF

PUBLIC SERVICE COMPANY OF COLORADO

August 2, 2016

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF COLORADO**

*** * * * ***

RE: IN THE MATTER OF THE APPLICATION OF PUBLIC SERVICE COMPANY OF COLORADO FOR AN ORDER GRANTING A CERTIFICATE OF PUBLIC CONVENIENCE AND NECESSITY FOR DISTRIBUTION GRID ENHANCEMENTS, INCLUDING ADVANCED METERING AND INTEGRATED VOLT-VAR OPTIMIZATION INFRASTRUCTURE	**))))))))))**	**PROCEEDING NO. 16A-____E**

SUMMARY OF THE DIRECT TESTIMONY OF DAVID C. HARKNESS

Mr. David C. Harkness is Chief Information Officer and Senior Vice President of Xcel Energy Services Inc. ("XES"). In this position, Mr. Harkness is responsible for the XES Business Systems organization, which provides Information Technology ("IT") services to XES and its operating company affiliates, including Public Service Company of Colorado ("Public Service" or "Company"). Mr. Harkness is also responsible for the corporate Business Continuity function and IT disaster recovery.

In his Direct Testimony, Mr. Harkness first presents an overview of the business systems and IT services that will integrate the various components of the Advanced Grid Intelligence and Security ("AGIS") initiative. Mr. Harkness also briefly describes the AGIS initiative, noting that it is a comprehensive plan that will make Public Service's electric distribution system more automated, resilient, and interactive by utilizing

advances in sensing, controls, information, computing, communications, materials, and components.

Mr. Harkness then discusses the IT infrastructure that will support all aspects of the AGIS initiative. He notes that while the main components of the AGIS initiative are described by other Company witnesses, supporting IT infrastructure and integration of the components of AGIS will allow new applications and field devices to communicate with and deliver data to the Company's "back office applications." In other words, IT enables the software applications that support the Company's customer service needs, billing, payment remittance, service order management, outage management, meter reading, and asset inventory lifecycle management applications to utilize the customer data, outage data, and other information supplied by the advanced distribution grid.

Mr. Harkness also describes the implementation plan for Public Service's IT integration efforts, noting that primary implementation is likely to begin in early 2017 and will continue for approximately 24 months. He discusses the anticipated costs associated with IT integration including cyber security support, and explains that IT efforts generally will not provide customers with benefits directly. Rather, IT support facilitates the intelligent, integrated nature of the advanced distribution grid. IT support is also necessary to facilitate certain customer interaction points, such as a customer internet portal that utilizes communications with advanced meters to provide near real-time energy usage information to customers.

Next, Mr. Harkness provides a discussion of the cyber security measures that will be needed to protect the more intelligent, interactive electric distribution network as well as the underlying data it gathers. He describes Xcel Energy's security principles, and explains the protection that will be implemented to secure customer endpoints and the communications network that facilitates the movement of data through the advanced grid. Overall, he explains how Public Service continually identifies and implements cyber security best practices to protect Public Service's customers and the electric distribution grid.

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF COLORADO

* * * * *

RE: IN THE MATTER OF THE APPLICATION OF PUBLIC SERVICE COMPANY OF COLORADO FOR AN ORDER GRANTING A CERTIFICATE OF PUBLIC CONVENIENCE AND NECESSITY FOR DISTRIBUTION GRID ENHANCEMENTS, INCLUDING ADVANCED METERING AND INTEGRATED VOLT-VAR OPTIMIZATION INFRASTRUCTURE	**)**	**PROCEEDING NO. 16A-____E**

DIRECT TESTIMONY AND ATTACHMENTS OF DAVID C. HARKNESS

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF ATTACHMENTS

GLOSSARY OF ACRONYMS AND DEFINED TERMS

Acronym/Defined Term	Meaning
ADMS	Advanced Distribution Management System
AGIS	Advanced Grid Intelligence and Security
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
ANSI	American National Standards Institute
BPL	Broadband over Power Line
C&I	Commercial and Industrial
CAIDI	Customer Average Interruption Duration Index
CBA	Cost-Benefit Analysis
CIS	Customer Information System
CMO	Customer Minutes Out
Commission	Colorado Public Utilities Commission
Company	Public Service Company of Colorado
CPCN	Certificate of Public Convenience and Necessity
CPCN Projects	AMI, IVVO, and the components of the FAN that support these components
CPE	Customer premise equipment
CRS	Customer Resource System
CSF	Cyber Security Framework
CVR	Conservation Voltage Reduction
DA	Distribution Automation
DDOS	Distributed Denial of Service
DER	Distributed Energy Resources
DOS	Denial-of-service
DR	Demand Response
DSM	Demand Side Management
DVO	Distribution Voltage Optimization
EPRI	Electric Power Research Institute
ERT	Encoder Receiver Transmitter
ESB	Enterprise Service Bus
FAN	Field Area Network
FLISR	Fault Locate Isolation System Restoration

Acronym/Defined Term	Meaning
FLP	Fault Location Prediction
GFCI	Ground Fault Circuit Interrupter
GIS	Geospatial Information System
HAN	Home Area Networks
ICE	Interruption Cost Estimation
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics
IPS	Internet Provider Security
IT	Information technology
IVR	Interactive Voice Response
IVVO	Integrated Volt-VAr Optimization
kVAr	Kilovolt-amperes reactive
kVArh	Reactive power
kW	Kilowatt
kWh	Kilowatt hours
LTCs	Load Tap Changers
LTE	Long-Term Evolution
MDM	Meter Data Management
MitM	Man-in-the-Middle Attack
MPLS	Multiprotocol Label Switching
NCAR	National Center for Atmospheric Research
NOC	Network Operations Center
NPV	Net Present Value
O&M	Operations and Maintenance
OMS	Outage Management System
OT	Operational Technology
PTMP	Point-to-multipoint
Public Service	Public Service Company of Colorado
RF	Radio frequency
RFP	Request for Proposal
RFx	Request for Information and Pricing
RTU	Remote Terminal Units

Acronym/Defined Term	Meaning
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	Supervisory Control and Data Acquisition
SGCC	Smart Grid Consumer Collaborative
SGIG	Smart grid investment grants
SIEM	Security Incident and Event Management
SVC	Secondary static VAr compensators
TOU	Time-of-use
USEIA	United States Energy Information Administration
WACC	Weighted Average Costs of Capital
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WiSUN	802.15.4g Standard
Xcel Energy Inc.	Xcel Energy
XES	Xcel Energy Services Inc.

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF COLORADO**

*** * * * ***

RE: IN THE MATTER OF THE APPLICATION OF PUBLIC SERVICE COMPANY OF COLORADO FOR AN ORDER GRANTING A CERTIFICATE OF PUBLIC CONVENIENCE AND NECESSITY FOR DISTRIBUTION GRID ENHANCEMENTS, INCLUDING ADVANCED METERING AND INTEGRATED VOLT-VAR OPTIMIZATION INFRASTRUCTURE	**))))))))))**	**PROCEEDING NO. 16A-____E**

DIRECT TESTIMONY AND ATTACHMENTS OF DAVID C. HARKNESS

I. INTRODUCTION, QUALIFICATIONS, AND PURPOSE OF TESTIMONY

Q. PLEASE STATE YOUR NAME AND BUSINESS ADDRESS.

A. My name is David C. Harkness. My business address is 414 Nicollet Mall, Suite 400, Minneapolis, Minnesota 55401.

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

A. I am employed by Xcel Energy Services Inc. (“XES”) as the Chief Information Officer and Senior Vice President. XES is a wholly-owned subsidiary of Xcel Energy Inc. (“Xcel Energy”), and provides an array of support services to Public Service Company of Colorado (“Public Service” or “Company”) and the other utility operating company subsidiaries of Xcel Energy on a coordinated basis.

Q. ON WHOSE BEHALF ARE YOU TESTIFYING IN THE PROCEEDING?

A. I am testifying on behalf of Public Service.

Q. PLEASE SUMMARIZE YOUR RESPONSIBILITIES AND QUALIFICATIONS.

A. As the Chief Information Officer and Senior Vice President ("CIO & SVP") Business Systems, I am responsible for the XES Business Systems organization, which provides Information Technology ("IT") services to XES and the Xcel Energy operating companies, including Public Service. In this role, I am also responsible for the corporate Business Continuity function and IT disaster recovery. A more detailed description of my qualifications, duties, and responsibilities is set forth after the conclusion of my testimony in my Statement of Qualifications

Q. WHAT IS THE PURPOSE OF YOUR DIRECT TESTIMONY?

A. The primary purposes of my testimony are to describe the Information Technology ("IT") and cyber security measures necessary to support the Company's proposal to advance the electric distribution grid. In particular, IT integration and cyber security protections are needed to support several new technologies on the grid, including two for which the Company is seeking a Certificate of Convenience and Public Necessity ("CPCN") in this proceeding: the Advanced Metering Infrastructure ("AMI") and the Integrated Volt-VAr Optimization ("IVVO"), as well as the components of the Field Area Network ("FAN") that support AMI and IVVO (collectively, the "CPCN Projects"). These technologies, as well as the Company's Advanced Distribution Management System ("ADMS"), and Fault Location Isolation and Service Restoration ("FLISR") function including the Fault Location Prediction ("FLP") component, are the critical parts of the Company's Advanced Grid Intelligence and Security

("AGIS") initiative. The AGIS initiative is a comprehensive plan that will advance Public Service's electric distribution system, provide customers with more choices, and enhance the way the Company serves its customers. AGIS will lay the foundation for an interactive, intelligent, and efficient grid system that will be even more reliable and better prepared to meet the energy demands of the future. A more thorough discussion of Public Service's AGIS initiative and the request to approve the Company's CPCN Projects Application is provided in the Direct Testimonies of Company witnesses Ms. Alice K. Jackson and Mr. John D. Lee.

Q. PLEASE SUMMARIZE YOUR TESTIMONY.

A. First, I provide an overview of the Company's information technology support services, discuss the IT underlying the AGIS initiative, and explain how IT is necessary for the overall system to function. I note that while the main components of the AGIS initiative are covered by other Company witnesses, supporting IT infrastructure and integration of the components of AGIS will allow these new AGIS field devices to communicate with and deliver data generated from field devices to the Company's "back office applications" that use the data in a variety of different applications. The term "back office applications" refers to other Xcel Energy software applications that support the Company's customer service needs, billing, payment remittance, service order management, outage management, meter reading, and asset inventory lifecycle management. While individual components of the AGIS initiative will each provide benefits to the Company, IT integration assists in maximizing the collaborative benefits.

Second, I provide the overview of how cyber security relates to the next generation of Public Service's advanced electric distribution network. As Company witness Mr. Lee testifies, advancing the distribution grid is a key component of Public Service's business strategy and ongoing transformation into a utility of the future. Protection of the intelligent grid and of our customers depends heavily on the security initiatives implanted for the grid and its various components. I describe Xcel Energy's security principles and the implementation of those security principles in the proposed AGIS initiative.

Q. ARE YOU SPONSORING ANY ATTACHMENTS AS PART OF YOUR DIRECT TESTIMONY?

A. Yes, I am sponsoring the following:

- Attachment DCH-1: AMI IT Cost Summary
- Attachment DCH-2: IVVO IT Cost Summary

.

II. INFORMATION TECHNOLOGY FUNCTIONS AND ACTIVITIES

Q. WHAT IS BUSINESS SYSTEMS?

A. Business Systems is XES' centralized IT organization, providing technology services to support all aspects of the operations of the Xcel Energy operating companies, including Public Service. In this era, it is hard to identify any aspect of our operations that Business Systems does not in some manner support.

Q. PLEASE DESCRIBE BUSINESS SYSTEMS' KEY FUNCTIONS AND RESPONSIBILITIES.

A. The key services Business Systems provides include:

- **Systems Control:** Technology support to our generation, transmission, and distribution business areas to enable management and operation of the electric and gas system. One of the systems that we maintain is the Outage Management System ("OMS"), which tracks customer outages and dispatches repair crews to restore service. Business Systems also supports the Supervisory Control and Data Acquisition ("SCADA") system, which is used to monitor the health of the electric transmission and distribution systems.
- **Technology Infrastructure:** Support for each employee's hardware and software needs, including the provision and maintenance of hardware such as computers, phones, and servers; maintaining and updating operating systems; and providing sufficient data storage capabilities.
- **Customer IT Support:** Hardware and software needed to facilitate interactions with Public Service customers. These activities include

maintaining the company website that provides important information to customers about outages, the status of their account, the Company's energy efficiency programs and rebates, and the Company's operations. Business Systems also maintains the Customer Resource System ("CRS"), which is the Company's customer information system of record, and which generates approximately 1.5 million billing statements to Public Service retail customers on a monthly basis. Business Systems also supports the Interactive Voice Response ("IVR") software that enables interaction with customers via telephone keypad or speech recognition.

- **Corporate IT Support:** Business Systems provides IT support for necessary corporate functions such as Human Resources and Financial Management. This includes maintaining software that enables creation, tracking, reporting, and analysis of financial and employee-related information.

Q. DOES XCEL ENERGY ALSO HAVE A CYBER SECURITY BUSINESS AREA?

A. Yes. In addition to Business Systems, the Company also has a dedicated Cyber Security business unit that provides protection from cyber security attacks, including but not limited to computer viruses. My Direct Testimony in this proceeding will discuss how Business Systems will support the integration of the various components of the AGIS initiative and will discuss our cyber security protections that will be implemented alongside this initiative.

III. IT SUPPORT for AGIS

Q. WHAT ROLE DOES INFORMATION TECHNOLOGY PLAY IN THE ADVANCED DISTRIBUTION NETWORK PUBLIC SERVICE PROPOSES TO ESTABLISH?

A. As discussed in great detail in the Direct Testimony of Company witness Mr. Lee, Public Service envisions an increasingly intelligent, automated, and interactive electric distribution system that utilizes advancements in sensing, controls, information, computing, communications, materials and components. This greater intelligence and automation is dependent on information technology to share and analyze information, integrate systems, and support the advanced infrastructure in a timely and efficient manner. In turn, through the AGIS initiative the more advanced distribution system will be able to better meet customers' energy needs, while also integrating new sources of energy and improving grid reliability.

Q. WHAT ARE THE FOUNDATIONAL PROGRAMS MAKING UP THE AGIS INITIATIVE?

A. Each of the foundational programs, or technical components, of the AGIS initiative is discussed in detail by our technical witnesses; therefore, I only summarize the components that need to be integrated by IT:

- **ADMS:** ADMS is the central platform that manages each of the other AGIS components by providing integrated operating and decision software and hardware to assist control room, field personnel, and engineers with the monitoring, control and optimization of the electric distribution system in near real-time. ADMS is discussed in more detail in the Direct Testimony of Company witness Mr. Chad S. Nickell.

- **AMI:** AMI meters are able to measure and transmit voltage, current, customer usage, and power quality data and can provide near real-time monitoring between the meter, the AMI head-end, and ADMS. "AMI head-end" is the software that facilitates the sending of commands to the field devices and receives the data back from the field devices. These meters also allow remote service disconnects and reconnects. All of these functions require IT integration between the AMI meters, AMI head-end, ADMS, and other Company systems. AMI is discussed in more detail in the Direct Testimony of Company witness Mr. Russell E. Borchardt.
- **FAN:** The FAN is the communications network that will enable communications between the communications infrastructure that already exists at the Company's substations, the AMI head-end, the ADMS, and new intelligent field devices. The FAN is discussed in more detail in the Direct Testimony of Company witness Mr. Wendall A. Reimer.

- **<u>IVVO:</u>** IVVO is a software application that automates the operation of the distribution voltage regulating and VAr control devices to reduce electrical losses, electrical demand, and energy consumption, and provides increased capacity to host Distributed Energy Resources ("DERs").[1]
- **<u>Geospatial Information System (“GIS”):</u>** GIS provides location information about all physical assets that make up the distribution system. GIS provides this data to ADMS to maintain the as-operated electrical model and advanced applications.

Q. WHAT WORK WILL BE REQUIRED OF BUSINESS SYSTEMS TO SUPPORT THE AGIS INITIATIVE?

A. Overall, Business Systems is responsible for integrating AGIS systems and data with other back office applications existing at the Company, as I describe in more detail below. Business Systems will implement new AMI head-end software. The AMI head-end software will be installed and configured to run on new server hardware. From the AMI head-end, interfaces will need to be built to transfer the data to other applications, such as ADMS, meter data management system, billing and customer service system, and the asset inventory management system.

[1] Additional intelligent field devices include Fault Location Isolation and Service Restoration (“FLISR”), Fault Location Prediction (“FLP”). FLISR involves automated switching devices to decrease the duration and number of customers affected by any individual outage. FLP is a subset application of FLISR that leverages sensor data from field devices to locate a faulted section of a feeder line and reduce patrol times needed to physically locate the fault. IVVO, FLISR, and FLP are discussed in more detail in the Direct Testimony of Mr. Nickell.

While the details of the interfaces will be determined in the design phase of the project, we know there will be requirements for the interfaces to transfer large volumes of data in a small amount of time. We also know that we will be obtaining significantly more data from the field devices than we have in the past. This additional data will require additional space for storage and a data management plan to ensure we are keeping the necessary data only for as long as it is needed. The new software, additional server hardware, and increase in quantity of data stored will all need to be supported, which will require an increase in our support staffs.

Q. TO WHAT EXTENT DOES BUSINESS SYSTEMS ANTICIPATE UPGRADES TO BACK-OFFICE APPLICATIONS AS A RESULT OF AGIS?

A. Until the Company is in the design phase of the AGIS program, we cannot fully identify and design the extent of back-office application upgrades that will be required. We know that the new AMI field devices will provide data we have not stored in our systems before, that this data will be in larger quantities than we have obtained before, and that effective use and communication of this data will require upgrades to many of our existing business processes.

Some examples of data that we have not received before from field devices are voltage and temperature readings. We will have larger quantities of data as we will be getting data from meters several times a day – and possibly more frequently by customer request through the customer data portal or smartphone application, as described in more detail below – whereas today we receive this data on a monthly basis. To support the new data and processes, the Company may have to upgrade a software application to accommodate new fields and increase the applications data storage capacity and processing. Once a meter vendor is selected, Public Service will have more information.

Due to the number of unknowns at this time regarding the specific design of different components of the AGIS initiative, a contingency has been added to the current cost estimates. Public Service anticipates refining its estimates once a meter vendor is selected and more information is available regarding the level and type of application upgrades that will need to be performed.

Q. WHAT IS "IT INTEGRATION"?

A. By IT integration, I refer to the need to integrate the technical components of the AGIS initiative (*i.e.*, the ADMS, FAN, FLISR, IVVO, GIS and AMI systems) with other Public Service applications to allow the efficient, timely, and secure transfer of data between the AMI system and other Public Service systems. The goal of integration is to ensure new applications and data are able to communicate with our existing applications so we are able to use the data to improve Public Service operations and provide a better customer experience.

As one example, AMI meter data must be communicated to the ADMS for operations and management of the grid, and back to back-office applications such as billing and customer care for the data to be used consistently and as effectively as possible. As the business processes are defined, the necessary data and applications requiring the new data gathered from the AGIS components will be identified. Interfaces will be designed to transfer the data between the applications. The new interfaces to support the new business processes will require significant labor to design and implement. We will need to use existing tools, such as an Enterprise Service Bus ("ESB"), to make the implementation and support of the interfaces more efficient.

Q. WHY DOES PUBLIC SERVICE NEED TO INTEGRATE THE COMPONENTS OF THE AGIS INITIATIVE WITH OTHER COMPANY SYSTEMS?

A. IT integration of the components of AGIS will allow the Company to obtain and communicate AMI data to back-office applications efficiently. As a result of systems integration, the processing of information will be automated. Integration will in turn support the Company’s ability to maximize the benefit of AGIS by significantly expanding the use of Operational Technology (“OT”), which is identifying or making an operational change based on information received. The information may come directly from, for example, a device or process. As the use of systems and OT matures, the Company will be able to use information from many different, integrated sources to assist in managing the electric grid and maximizing the benefits of AMI for our Colorado electric customers.

Q. HOW WILL AMI AND BACK OFFICE APPLICATIONS BE INTEGRATED?

A. Public Service will connect the AMI meter with the AMI head-end software that sends commands to meters and receives data from the meter using the FAN for communication. From the AMI head-end, data will be distributed to other back office applications, likely using an ESB, to enable the capabilities to deliver benefits to the Company and its customers.

Q. WHAT APPLICATIONS WILL BE INTEGRATED WITH AMI?

A. The following applications will be integrated so they can use AMI data:

1. **ADMS:** As previously noted, ADMS will provide an integrated operating and decision software support system to assist control room, field personnel, and engineers with the monitoring, control and optimization of the electric distribution system, as summarized in the Direct Testimony of Company witness Mr. Lee and discussed in detail by Company witness Mr. Nickell. ADMS will use the AMI data to deliver business capabilities, such as IVVO and FLISR.
2. **Customer Information System ("CIS"):** The application provides capabilities for customer service, billing, service orders, and payments. The Customer Information System ("CIS") is currently integrated with the Meter Asset Lifecycle Management System and Meter Data Management ("MDM") System. AMI head-end integration with the CIS will allow Public Service to streamline multiple processes. As an example of a process improvement resulting from integrating the AMI head-end with the CIS, we will be able to obtain a meter reading to begin or end the billing when a customer moves into or out of a premise without a visit to the customer's premise. As another example, when a customer is delinquent in paying their bill, the Company will be able to issue an order from the CIS to the AMI head-end to request the customer's service be disconnected. When a disconnected customer pays their bill, an order generated in the CIS will be sent to the AMI head-end to reconnect the service. Disconnect and

reconnect processes today are manual processes that require a person to physically visit the customer's site.

3. **Meter Asset Lifecycle Management System:** This system manages the entire life cycle of serialized metering devices, including purchasing, testing, field installation location, field removal, and retirement of the asset. The Meter Asset Lifecycle Management System is currently integrated with the MDM System and CIS. The new integration of the AMI head-end with the Meter Asset Lifecycle Management System will allow it to remain as the Company's primary source of location information and attributes for serialized metering devices. The AMI head-end will receive the meter location and attribute information to enable provisioning of the meter, understand its location, and obtain data from the meter.

4. **MDM:** This system provides capabilities to validate, edit, and estimate meter readings and manages events from the meter, such as power outages and tampering. The MDM will also assist in facilitating communication to and receiving data back from the AMI head-end. The MDM is currently integrated with the Meter Asset Lifecycle Management System and CIS. AMI will significantly increase the number of meters and amount of data loaded to our MDM. The MDM will serve as the central repository for the reading data. The MDM will also validate the meter data and export it for use in billing, customer viewing, and analytics.

5. **Customer portal:** The portal is used by customers to obtain account information, such as billing and meter reading history. The customer

portal is currently integrated with the CIS and MDM. AMI data from field devices will move through the AMI head-end to the customer portal, where customers will have the ability to see more granular meter reading data than they see today.

While our final design has not yet been determined, our current customer portal design plan will provide routine meter readings, which will be obtained from the meters several times a day and will provide the majority of data that is shown when customers request a display of their usage by time interval. In addition, to ensure the customer is provided with the most up to date information, the data from the routine meter readings will be supplemented with the latest information available from the meter. This will be done automatically by the customer portal sending an “on demand” read request to the meter, obtaining the latest readings from the meter, and then combining this new data with the data obtained from the routine reading process for customer viewing. In addition, the customer portal will provide the customer with the option of “refreshing” the information on the screen through a similar process. A smartphone application will also provide customers with similar capabilities.

The applications referenced above will share data with other applications, such as the Company’s Data Warehouse, as well as new Distribution Analytics software.

Q. DESCRIBE THE COMPANY'S DATA WAREHOUSE AND DISTRIBUTION ANALYTICS SOFTWARE.

A. The existing Data Warehouse is used to consolidate data from separate systems of record to facilitate efficient generation of reports and perform analysis of the data. The Distribution Analytics Software will be new to the Company. The Distribution Analytics Software is expected to receive data from the AMI head-end, Meter Data Management System, and the Customer Information System. The Distribution Analytics Software is expected to use the data to perform analytics to identify trends for such items as reverse flow, tampering, load side voltage, and temperature. Once specific data analysis needs are defined and the software is selected, integration details will be defined.

Q. WHAT ARE THE IMPACTS IF PUBLIC SERVICE DOES NOT MAKE THE INVESTMENTS NECESSARY TO INTEGRATE AGIS COMPONENTS WITH BACK-OFFICE APPLICATIONS?

A. Without integrating the technical components of the AGIS initiative with other Public Service applications, Public Service will not be able to take advantage of the benefits and capabilities of the new AGIS components. Each application provides a new capability and benefit to the Company. Without integration, existing applications would not be able to request data from new field devices, such as AMI meters, and the data provided from these new field devices would not be able to be communicated, stored, or analyzed by our existing applications. In addition, a lack of integration would cause many processes to be manual, and would not allow the ability to make decisions based on recent data collected, all of which will reduce the benefits of these technologies, especially AMI.

For example, when a customer moves into a new site, without integration a Customer Contact representative would need to generate a list of orders from the CIS, log into the AMI head-end, execute the command to read the meter, wait for the result, and complete the order in the CIS. With integration, the move-in order would automatically transfer to the AMI head-end, be executed, and results sent to the CIS for completion of the order, with no manual intervention. Another example where integration will reduce manual processes and add efficiency is for disconnects and reconnects of the customer's electric service, as previously noted. If Public Service did not integrate the CIS to the AMI head-end, orders generated in the CIS to disconnect or reconnect the meters would not transfer to and be executed by the AMI head-end automatically. Rather, Customer Contact Center employees would need to generate a list of the orders from the CIS, log into the AMI head-end, execute the command, wait for the result, and complete the order in the CIS.

Q. OTHER THAN INTEGRATION, WHAT OTHER WORK WILL BUSINESS SYSTEMS PERFORM?

A. The AMI head-end software application will need to be installed and configured on new Public Service hardware. The new application will also need to be setup for data backups, disaster recovery, security, purge and archive of data, and have a support plan generated. In addition, a review of existing applications, such as the MDM, will need to be performed to ensure the applications will be able to properly import, process, and export the significantly larger volumes of data we will be receiving from the field devices. Existing applications may need to have additional storage allocated to them and may need to have additional processing power added to the servers to maintain application performance.

Q. WILL THE COMPANY PERFORM THE SYSTEM INTEGRATION WITH EXISTING RESOURCES?

A. Due to the large volume of work expected to occur within 24 months, Public Service will need to hire a third-party firm to supplement our existing IT resources. Estimates of costs for vendor IT work associated with AMI and IVVO are part of our CPCN Projects, with IT cost estimates described below.

IV. IMPLEMENTATION

Q. WHAT IS THE TIMELINE FOR IMPLEMENTATION OF THE BUSINESS SYSTEMS APPLICATION INFRASTRUCTURE YOU HAVE DESCRIBED?

A. Public Service has documented an assumption of 24 months, consisting of several phases, to implement the Business Systems application infrastructure and interfaces to integrate the AMI head-end with other the Company applications. The 24 months is expected to begin after vendor contract execution, which we expect to occur in the first half of 2017.

Q. WHAT IS THE NEXT STEP AFTER CONTRACT EXECUTION?

A. Xcel Energy will move into the Planning phase, which includes completing high level and detailed designs, creating network, infrastructure, and security models, training plans, disaster recovery plans, and a test strategy. This phase also includes refining the timeline, cost, and benefits based on new learnings. The Planning phase is expected to take approximately twelve months.

Q. WHAT IS THE NEXT STEP AFTER THE PLANNING PHASE?

A. We will move into the Execution phase, which includes creating detailed test plans, configuring test systems, performing testing, and implementing the solution. This phase also includes refining the timeline, cost, and benefits based on the additional details that will be available at that time. The Execution phase is expected to start about six months after the Planning phase begins and will last for approximately 18 months. The overlap of the two phases will allow the Execution phase to begin for items that have completed the Planning phase, which assists in shortening the overall project timeline.

Q. WILL ALL IT BUSINESS CAPABILITIES BE DELIVERED WITHIN THE 24 MONTHS?

A. There is an assumption that not all business capabilities will be delivered at one time, but sufficient capabilities will be delivered within the 24 months to allow the installation of AMI meters. Business Systems will work with business areas to prioritize the capabilities and will implement based on the cost and benefit of each capability.

Q. COULD THIS IMPLEMENTATION SCHEDULE CHANGE?

A. While believe that our IT implementation schedule is reasonable, it is possible the IT work plan will evolve. This project is in its early stages and we are using current information to generate the timelines included in this filing. As the project progresses and more details are identified, such as a vendor selected, detailed requirements documented, and the solution design completed, the timeline will be refined and could change from what is presented here.

V. COSTS AND BENEFITS

Q. FOR THE TECHNOLOGIES INVOLVED IN THIS CPCN APPLICATION, WHAT IT INTEGRATION COSTS DOES PUBLIC SERVICE ESTIMATE?

A. My Direct Testimony will address the IT integration costs for the AMI and IVVO components of the AGIS initiative. Attachment DCH-1 to my Direct Testimony summarizes the estimated capital and O&M costs for the IT applications and integration for the AMI meters to be deployed as part of the AGIS initiative. Attachment DCH-2 to my Direct Testimony summarizes the estimated capital costs for the IT applications and integration for the deployment of the IVVO technology as part of the AGIS initiative.

Company witness Mr. Samuel J. Hancock testifies in detail about the cost-benefit analysis for the CPCN Projects, and his Direct Testimony and attachments summarize and compare the costs and benefits estimated for the various foundational components of the AGIS initiative for which approval is sought in this CPCN application.

Q. WHAT ARE THE TOTAL IT INTEGRATION COSTS?

A. The capital costs for IT Integration for the AMI and IVVO technologies, for which approval is sought in this application, are estimated to be $67.5 million, with an additional estimated $55.9 million for contingency.

Q. OVER WHAT TIME PERIODS WILL IT INVESTMENTS NEED TO BE MADE IN SUPPORT OF AMI AND IVVO?

A. Primary IT investments will be needed through the major project implementation period of 2016 through 2021, as illustrated in Attachments DCH-1and DCH-2. However, information technology software typically requires upgrades and replacements more frequently than other assets due to changes in technology, vendor support gaps for aged software, and evolving cyber security requirements. Therefore, we anticipate periodic additional IT capital investments through the life of the AMI meters (approximately 2035), as depicted by Company witness Mr. Hancock's CBA.

Q. WHAT ARE THE INTEGRATION COSTS FOR AMI?

A. The capital costs for IT Integration for AMI are $50.9 million, with an additional estimated $50.9 million for contingency. The AMI IT costs include hardware, which covers items like, but not limited to, servers and firewalls. As I noted earlier in my testimony, AMI IT software costs include the purchase of AMI head-end and Distribution Analytics software, as well as an increase in licensing for our existing Meter Data Management System. The labor costs include documenting requirements, vendor selection, design, implementation of the solution, and one future software upgrade.

Q. WHAT ARE THE INTEGRATION COSTS FOR IVVO?

A. The capital costs for IT Integration for IVVO are $16.6 million, with an additional estimated $5.0 million for contingency.

Q. ARE THERE ON-GOING IT OPERATING COSTS ASSOCIATED WITH AMI AND IVVO?

A. Yes. The estimated IT Operation & Maintenance ("O&M") costs for 5 years for these same technologies are estimated to be $14.6 million, with another $14.6 million for contingency. The AMI O&M IT costs include hardware support, data storage, annual software maintenance, and labor for software support. There are no IVVO O&M IT costs apart from the ADMS application support, which is not part of this filing.

Q. HOW WERE THE HARDWARE COST ESTIMATES DEVELOPED?

A. The Company developed the cost estimates for hardware based on sample hardware requirements provided by software vendors, internal costs to deploy the hardware, and existing hardware support costs. To obtain sample hardware requirements from software vendors, Public Service provided high level project information, such as volume of meters and data, and the vendors replied with high level information regarding the quantity and specifications for the hardware. Public Service applied costs to the quantity and specifications based on other similar hardware purchases and existing costs to support the hardware to generate the estimate.

Q. **HOW WERE THE SOFTWARE COST ESTIMATES DEVELOPED?**

A. The software cost estimates are based on an average of indicative costs from a Request for Information and Pricing ("RFx") sent to four AMI vendors, as well as on existing vendor licensing costs. The RFx was conducted by the Company as a means to gather information from potential AMI vendors on representative solutions and costs.

Q. **WHAT WERE THE INPUTS USED TO GENERATE LABOR COST ESTIMATES?**

A. Input for labor costs included the estimated number of application integrations needed, assumed project duration, application and interface support, vendor consultation, employee travel, and project management needs.

Q. HOW WERE THE NUMBER OF INTEGRATIONS ESTIMATED?

A. To estimate the number of application integrations needed, Xcel Energy reviewed AMI head-end documentation to understand what interfaces are available from the software, identified what other applications would need to use the interfaces, and applied average interface build costs to generate the cost estimate.

Q. HOW WAS THE PROJECT DURATION ESTIMATED?

A. Xcel Energy used an assumed project duration for integration of 24 months. The estimated duration is discussed earlier in this testimony.

Q. HOW WERE THE APPLICATION AND INTERFACE SUPPORT COSTS ESTIMATED?

A. Since there will be new integrations and software implemented as part of this project, average costs were added for additional support of four full-time equivalent employees.

Q. HOW WERE THE VENDOR CONSULTATION COSTS ESTIMATED?

A. The Company estimates there may be a need for vendor resources to support our project or make changes to their software. We assumed seven contracts with vendors with an average cost of $500,000 each.

Q. HOW WERE THE EMPLOYEE TRAVEL COSTS ESTIMATED?

A. The Company assumed that an average of five employees would incur average travel costs of $1,500 a week for the 100 weeks of the project.

Q. HOW WERE THE PROJECT MANAGEMENT TRAVEL COSTS ESTIMATED?

A. Project Management costs are based on the need for a Project Manager, Business Analysts, and Project Coordinator for the project. For each of the resources, average duration and cost from previous projects was used.

Q. HOW WERE THE CONTINGENCY AMOUNTS DETERMINED?

A. This project is in its early stages. During the early stages of a project, high level information is used as an input to generate a high level cost estimate, which is what is included in this filing. As the project progresses and more details are identified, such as a vendor selected, detailed requirements documented, and the solution design completed, the cost estimates will be refined and the specific project cost risks will be identified. As the additional detail is identified to eliminate the risk, the contingency estimate will be refined and reduced. The Company will provide updated costs in this proceeding after the vendor contract is executed.

Q. FOR THE TECHNOLOGIES INVOLVED IN THIS CPCN APPLICATION, WHAT IT INTEGRATION BENEFITS DOES PUBLIC SERVICE ESTIMATE?

A. The benefits of IT Integration are inherent in the implementation of the individual technologies of the AGIS initiative; therefore, I understand that Mr. Hancock's Direct Testimony and attachments do not include a discrete benefit estimate for IT Integration for the AMI and IVVO technologies. As AMI rolls out across our enterprise, we will eventually be able to retire legacy meter reading applications to save those costs for customers. However, the existing meter reading applications will continue to be used for gas meters in Colorado as well as electric and gas meters in other jurisdictions until grid advancement becomes more enterprise-wide in the coming years.

Overall, IT infrastructure and integration are necessary to the successful implementation of the AGIS components; therefore, the benefits of IT efforts are largely subsumed by other aspects of the AGIS initiative, and these benefits could not be achieved without IT integration.

VI. DISTRIBUTION GRID SECURITY

Q. WHAT IS THE OVERALL ROLE OF CYBER SECURITY WITHIN THE AGIS PLAN?

A. The role of cyber security within the AGIS plan is to help ensure all components of the intelligent grid are identified and protected, both for the protection of customers and for the reliable and safe delivery of energy to customers. Additionally, cyber security should validate that there are sufficient detective controls at strategic locations to provide early notification of suspicious behavior or anomalous activity. Furthermore, appropriate levels of response must be planned, refined and exercised to react appropriately to all possible threats to the intelligent grid.

Q. WHAT SECURITY RISKS ARE ASSOCIATED WITH THE TECHNOLOGIES PROPOSED AS PART OF THE AGIS INITIATIVE?

A. In my opinion, the security risks associated with the AGIS components are the potential compromise of the communication devices or the compromise of the channel between the consumer and the control center. As communications technology has become more advanced and carried more detailed information in recent years, the disruption of communications is a fundamental risk of any network. With respect to the distribution grid, a compromise of the channel between the consumer and the control center could lead to disruption of information, data integrity, or even of the distribution control center. Therefore, protecting the integrity of the communication devices and channels that allow the advanced grid to perform at expected levels is paramount. It is also important to implement the correct level of monitoring and alerting, configured to identify potentially anomalous activity, so that both proactive and reactive responses are appropriate and efficient.

Q. DOES THE COMPANY EMPLOY BEST PRACTICES FOR CYBER SECURITY?

A. Yes. As Public Service moves forward into the next generation of intelligent electric distribution, each and every facet of this electric network must be scrutinized and evaluated for cyber security risk. While reliable delivery of electricity is of paramount importance, protecting the integrity of this system is part of that responsibility. Therefore, all aspects of the advanced distribution system must be inventoried, securely configured, and monitored regularly and thoroughly to protect Xcel Energy and our customers from Cyber Security threats.

A. <u>Cyber Security Principles</u>

Q. IN YOUR OPINION, WHAT ARE THE BEST CYBER SECURITY PRACTICES FOR XCEL ENERGY?

A. There are four main principles to which Xcel Energy, and its operating utilities like Public Service, needs to adhere in order to best protect the intelligent electric distribution network. The first is a “defense-in-depth” defense, which ensures there are multiple layers of protection and detection defined within the distribution grid advancement effort. This includes defenses at each endpoint, throughout the communication network, at the entrance to the distribution control centers, at all authentication and authorization points and then providing a robust monitoring and alerting system to notify appropriate personnel in the event of anomalous or suspicious activity.

Second is the principle of “zero-trust”. This concept creates isolation points within the information network so that only specific hosts are able to communicate with other specific hosts. This requires granular segmentation and tight communication rules so that only valid communication is received and acted upon.

The third principle, “least privilege”, builds upon the first two in that only necessary individuals and services are allowed to interact with devices on the intelligent electric distribution network. Strong authentication must exist to validate administrative users and the concept of “least privilege” is applied to all users and services running on the devices. Least privilege means that users or services only receive the permissions to perform functions that they need to perform their duties. This limits the exposure to systems or devices if an account is compromised.

The last principle is similar to the third in that systems and devices are configured to match “least functionality.” Least functionality does not mean minimum service or function overall, but rather that only necessary ports and services are open and running on the systems and devices to minimize the exposure point of any discovered or undiscovered (zero-day) vulnerabilities. This decreases the threat profile of the environment and reduces a potential exposure should a vulnerability be identified for an unnecessary, disabled service.

Q. HAS XCEL ENERGY IMPLEMENTED THE CYBER SECURITY BEST PRACTICES THAT YOU DESCRIBED?

A. Yes. These cyber security principles will be applied to the technology to be implemented as part of the AGIS initiative to identify and protect all components of the intelligent grid and help ensure the reliable and safe delivery of energy to Public Service's customers. In addition, Xcel Energy has implemented several Endpoint Protections to achieve the first principles of cyber security that are described above.

B. <u>Endpoint Protections</u>

Q. WHAT IS "ENDPOINT PROTECTION?"

A. Endpoint Protection is the installation and/or enablement of protective and detective cyber security controls to thwart malware and external influences from causing unexpected, unwanted or invalid behavior at a communication endpoint. This includes the AMI meter and head-end, but also includes any communication device such as routers or switches that could be used to exploit the network. If such behavior exists, the detective controls should immediately notify appropriate personnel so that appropriate responses can occur. This may include repairing of necessary communication or functionality, but could potentially include the replacement of the endpoint.

Q. WHAT TYPES OF ENDPOINT PROTECTION HAS XCEL ENERGY IMPLEMENTED?

A. Xcel Energy's Endpoint Protections include: (1) Access Control; (2) Authentication and Authorization; (3) Authorized Protocols; and (4) Data

Validation and Protection. These endpoint protections are specified as cyber security controls in the AMI vendor selection process, as they are essential to protect the devices and the data that are handled by AMI meters and headend servers. Authentication and Authorization is integral to Access Control for any type of endpoint so that logical access to endpoints can only be performed by duly authorized personnel. By requiring endpoints to be configured with Authorized Protocols, best cyber security practices are maintained to the principle of least functionality mentioned above.

Q. PLEASE DESCRIBE "ACCESS CONTROL."

A. The first item of protection, Access Control, is to confirm that only necessary and authorized users have access to the individual devices. This not only includes the devices that are installed on the consumer's premises, but also the devices that facilitate communication and control of the data flowing to the consumer. There are potentially many avenues of compromise with respect to unauthorized access to devices. This is a key consideration and will be addressed through strong authentication methods, which include multi-factor authentication methods described below.

Q. PLEASE DESCRIBE "AUTHENTICATION AND AUTHORIZATION."

A. Xcel Energy must ensure that a least-privilege approach is taken for users and systems that have a need to authenticate to the devices. Granting undue permissions to devices that comprise the intelligent electric distribution system could lead to unauthorized changes and instability. All access to endpoints that make up the intelligent electric distribution system must comply with a least-privilege principle to ensure that only necessary and authorized individuals have the ability to make administrative changes.

Q. PLEASE DESCRIBE "AUTHORIZED PROTOCOLS."

A. Authorized Protocols, another item of significant importance, ties to the concepts discussed above of authentication and authorization. This concept is endpoint validation. This principle will ensure that only authorized devices have the ability to communicate with other authorized devices. A key concept of the intelligent electric distribution network is for edge devices to communicate to a central system or control center. To protect system integrity, only authorized devices must be allowed to communicate to other authorized devices. Allowing non-authenticated or validated devices to communicate to these components could lead to a denial-of-service ("DOS"), Man-in-the-middle attack ("MitM"), or potentially the compromise of a system or device.

DOS is any unintended disruption of service. While many people are familiar with a Distributed Denial of Service ("DDOS"), which is the use of many hosts (voluntary or involuntary) to flood a target device with valid or invalid communication that prevents the legitimate use of said device, disruption of a service could be caused by a multitude of factors. Similarly, a MitM attack is the interception and manipulation of communication as it passes between two valid hosts.

While there is a layered approach to protecting each one of these attacks, authorization of devices is one of the key layers of defense.

Q. PLEASE DESCRIBE "DATA VALIDATION AND PROTECTION."

A. A final defensive layer between the various endpoints is data validation. As data is sent from endpoints at consumer premises, data validation at the control center must take place. If data values received from the consumer endpoint do not match any expected values, then either the data must be assumed compromised and discarded, or secondary validation must take place to measure the integrity of the data received. This validation will provide yet another level of detection and protection for the intelligent electric distribution system.

As described above, each of these endpoint protections will support the overall security of the AGIS technology.

C. Communication Network Security Protections

Q. AS PART OF IMPLEMENTING CYBER SECURITY, DOES THE COMMUNICATION NETWORK ALSO NEED TO BE PROTECTED?

A. Yes. The communication network that facilitates data movement from the endpoint at the consumer premise to the utility's control center must also have a high level of security built into the architecture to ensure confidentiality, integrity, and availability of the intelligent electric distribution network.

Q. WHAT ARE THE PROTECTIONS XCEL ENERGY APPLIES TO THE COMMUNICATION NETWORK?

A. As with the consumer endpoint devices, the equipment that makes up the communication network will adhere to a least privilege authentication and authorization model. Only personnel with a specific business need will have the ability to authenticate to the communication network devices. Once authenticated, authorization privileges will be least required to perform the job duties assigned to those individuals or services. This is similar to the endpoint protection mechanisms, in that it protects the communication network in the event of compromised credentials for non-authorized individuals.

Q. ARE THERE OTHER LAYERS OF DEFENSE FOR THE COMMUNICATION NETWORK?

A. Yes. Another layer of defense with regards to authentication will be the requirement for multi-factor authentication to these devices. This will assist if administration credentials are compromised and access to these devices is attempted from a non-authorized endpoint. If such an attempt would occur, logging and monitoring, which I will discuss in greater detail below, will alert appropriate personnel to investigate.

Adhering to the Zero-Trust model, network devices will only be authorized to communicate to other network devices, endpoints or systems for which they have a need and specific authorization. This will isolate and segment the distribution network so only those devices that have a specific need to communicate will have that ability. This Zero-Trust model safeguards systems on different distribution networks so that a compromise of one distribution network does not lead to the compromise of others.

Q. DOES PROACTIVE LOG MONITORING HAVE A ROLE IN THE DEFENSE OF THE COMMUNICATION NETWORK?

A. Yes. Each device that resides on the intelligent electric distribution network must have the ability to log various pieces of information and send those logs to an intelligent collector, such as a Security Incident and Event Management ("SIEM") system. This system will collect, analyze, report, and alert on various activity. Some of this activity will be normal events and will be archived for reporting purposes. Other items, such as anomalous activity and known bad events, will create alarms, which will be sent to personnel responsible to investigate and take action upon those events. In all cases, log data will be retained for an appropriate period of time to ensure any auditing activities will have sufficient data to perform a satisfactory review.

Q. DOES PROACTIVE CHANGE MONITORING HAVE A ROLE IN THE DEFENSE OF THE COMMUNICATION NETWORK?

A. Yes. Change review and control will be another principle that must be holistically managed within this environment. Without a sufficient level of oversight and change governance, the integrity and security of individual devices, and ultimately the network, could be impacted. The absence of a sufficient level of oversight and change governance could result in the loss of information, disruption of communication, or an impact to the integrity of the data. Therefore, strict adherence to change management and change discovery will be incorporated into this effort.

Q. DOES EVERY COMMUNICATION CHANNEL OR MEDIUM NEED TO HAVE THE SAME LEVEL OF PROTECTION?

A. Yes. In order to ensure an efficient and holistic approach is taken to the intelligent electric distribution network, it must be Layer-1 agnostic. This means that the intelligent electric distribution network must interoperate with all available communication mediums, such as microwave, satellite, radio, cellular, T1 or Multiprotocol Label Switching ("MPLS") networks. The equipment that facilitates the specific communication medium must not impede the security controls placed on any of the equipment identified above. Therefore, all security controls should work independently of the specific communication medium.

In order to guarantee that every communication medium will offer the same level of protection, all data communication over these mediums will be validated and encrypted. As specified above, each device that needs to communicate to the other will be validated. In addition, the communication that travels over these links (microwave, radio, cellular, etc.) will be encrypted at the security devices that immediately precede the communication mechanism in order to remove any interoperability dependencies with these devices.

Q. DO ANY PROTECTIONS NEED TO BE APPLIED TO ACCESS TO DISTRIBUTION CONTROL CENTERS?

A. Yes. As communication flows from the consumer endpoint devices into the distribution control centers, the same level of security and protection must be applied. All access to the distribution control centers will follow the same rules for authentication, authorization, and least privilege.

Q. WHAT ARE THOSE PROTECTIONS?

A. All communication streams that seek access to the distribution control centers must be validated to ensure that these devices are trusted and verified. No unauthorized endpoints or communication devices will be allowed to communicate with the distribution control centers. Once authenticity has been validated, these devices will be able to communicate on approved protocols only. The data contained within these protocols should also be validated to ensure that all values are within expected ranges. If data values received from the consumer endpoint does not match expected values, then either the data must be assumed compromised and discarded, or secondary validation must take place to measure the integrity of the data received. If the data values cannot be validated, then an alert must be generated to investigate the cause for the unexpected values.

In order to ingest data from the intelligent electric distribution network to the distribution control center successfully, multiple defense-in-depth controls must be successfully passed. Communication will pass through a firewall to ensure that only authorized devices are communicating on authorized ports/protocols. Additionally, a protocol-aware Intrusion Detection System / Internet Provider Security ("IDS/IPS") will inspect the traffic to ensure tampering has not been performed on the packet. Successful transmission through these controls will also ensure that delivery of the information will be made to devices that are authorized to accept the data – and to none others. Once the data has been delivered to the systems responsible for consuming this information, only authorized processes will have the ability to act upon this information.

Q. DOES LIFE-CYCLE MANAGEMENT OF DEVICES HAVE A ROLE IN THE COMPANY'S IMPLEMENTATION OF CYBER SECURITY BEST PRACTICES?

A. Yes. The overall success of cyber security within the intelligent electric distribution network will be dependent upon the life-cycle management process of the equipment that makes up this network. Safeguarding this equipment is dependent upon an accurate inventory of all devices that enable this solution. Furthermore, each device must have a known and valid configuration.

Q. HOW WOULD LIFE-CYCLE MANAGEMENT OF DEVICES BE ACCOMPLISHED?

A. Continuous monitoring of the devices that comprise this solution must also be in place to validate appropriate and expected behavior of the system. If unexpected values occur, or if anomalous behavior occurs, it is imperative that trained personnel investigate the values or behavior to determine if this is a valid response or if the system is not behaving in an appropriate manner. If the anomalous activity is determined to be valid, then these personnel need to ensure the system is updated to expect these values under specified circumstances. Otherwise, these personnel need to investigate the activity and take appropriate action to remedy the response.

Additionally, proactive management of security updates to each piece of equipment that comprises this intelligent electric distribution network is imperative to protect the integrity of this network and security mechanisms put in place to secure it. Firmware and software updates must be regularly discovered, tested, and applied to ensure the system continues to deliver and perform at a very high level.

Q. DO MONITORING AND ANALYSIS OF COMMUNICATIONS HAVE A ROLE IN THE COMPANY'S IMPLEMENTATION OF CYBER SECURITY BEST PRACTICES?

A. Yes. Continuous monitoring of this solution is important to ensure the integrity and security of the system. As conditions change within the distribution network, Distribution Operators will closely monitor the values to ensure continuous and reliable delivery of electricity to our consumers. So too must the cyber security personnel provide continuous monitoring of this environment to verify the continuous and reliable operations of the equipment responsible for the delivery of electricity.

Q. HOW WOULD CONTINUOUS MONITORING BE ACCOMPLISHED?

A. To this end, all devices that comprise the intelligent electric distribution network must have the ability, and be configured, to send device logs to a SIEM system. This system will then be configured to detect and alert on anomalous activity. If such activity occurs, notification will be made to appropriate personnel who will then investigate and respond with the proper action.

Q. WOULD OTHER ITEMS NEED TO BE MONITORED AND EVALUATED TO ENSURE THE SECURITY OF THE INTELLIGENT ELECTRIC DISTRIBUTION SYSTEM?

A. Yes. Data integrity is also an item that must be monitored and evaluated, as was addressed above. By confirming the returned data values fall within an expected range, the integrity of the distribution control system can be maintained. Injecting bad data is a mechanism used to compromise the integrity and availability of a system without actually taking direct control over it. This would be a potential indicator of compromise to the intelligent electric distribution network and an immediate investigation would need to commence to verify whether a real attack is occurring or has occurred. Overall, each and every component that facilitates the measurement of electricity, the communication of this data and the control of the electricity to consumer premises must be monitored to provide the greatest value and reliability to Public Service and to its consumers.

Q. DO YOU HAVE ANY SEPARATE COST ESTIMATES FOR THE IMPLEMENTATION OF CYBER SECURITY FOR THE AGIS INITIATIVE?

A. No. The costs estimates for the IT integration with AGIS, which I discussed earlier in this testimony, include costs for deployment of cyber security as part of the AGIS initiative. Cyber security costs are part of the application development and integration efforts described above.

Q. WHAT ARE YOUR CONCLUSIONS REGARDING CYBER SECURITY WITH RESPECT TO AGIS?

A. My conclusion regarding cyber security of the intelligent electric distribution system is that there are real benefits to advancing the technology of the electric distribution grid. However, increasing the intelligence of the grid also presents tangible risks. Each one of those risks have been realized in organizations that have implemented similar technologies. The controls I discussed above will help protect both the consumer and the distribution network, detect attacks or attempted compromise occurrences, and respond in a timely manner to limit and/or prevent impact to the consumers or to Xcel Energy and Public Service.

These cyber security controls are seen as a best practice, and align with the Cyber Security Framework ("CSF") to Identify, Detect, Protect, Respond and Recover to known and unknown risks.

Q. DOES THIS CONCLUDE YOUR TESTIMONY?

A. Yes, it does.

Statement of Qualifications

David C. Harkness

I am the Chief Information Officer and Senior Vice President, for Xcel Energy Services Inc. I am responsible for the XES Business System organization, which provides Information Technology ("IT") services to XES and its operating company affiliates, including Public Service Company of Colorado. I am also responsible for the corporate Business Continuity function and IT disaster recovery.

I have 28 years of experience in the field of IT, with 24 of those years in a management role. I joined Xcel Energy in November 2009, following six years at PNM Resources at Albuquerque, New Mexico, where I first served as Senior Director, Business Process Outsourcing, then as Senior Director of Business Transformation and finally, as Vice President and CIO for more than three years. While in New Mexico, I was also appointed by Governor Richardson to New Mexico's Information Technology Commission, where I helped establish and direct the IT Strategy for the State of New Mexico. Prior to that experience, I held several IT Leadership roles for McLeod USA, MCI, and Rockwell International, where I began my career in 1986.

I graduated from the University of Iowa where I earned a Bachelor of Science degree in Computer Science and a Bachelor of Arts degree in Applied Mathematics.