BEFORE THE MISSOURI PUBLIC SERVICE COMMISSION

In the Matter of a Working Case to Address Security Practices for Protecting Essential Utility Infrastructure	)))	File No. AW-2015-0206

ITC MIDWEST LLC'S RESPONSE TO THE COMMISSION'S AUGUST 5, 2015 ORDER DIRECTING FILING

ITC Midwest LLC ("ITCMW"), for its Response to the Commission's August 5, 2015 Order Directing Filing, submits as follows:

Background

On August 5, 2015, the Missouri Public Service Commission ("Commission") directed regulated electric utilities, including ITCMW, to answer 22 questions (some with subparts) regarding cybersecurity practices.

ITCMW's response ("Response"), set forth below, restates each question the Commission asked and then follows with ITCMW's Response.

1. Does your company participate in an internal or external critical infrastructure or cybersecurity vulnerability assessment? If yes,

   a. Is the assessment conducted by a qualified independent third party and if so, by whom?

Response:

Yes. The assessment is conducted annually by a qualified independent third party. Last year, the assessment was performed by Viopoint, a company that specializes in penetration testing, phishing attempts, and social engineering.

2. If your company has deployed Advanced Metering Infrastructure (AMI), does your company have independent security audits conducted on a periodic basis?

Response:

ITCMW does not employ Advanced Metering Infrastructure. ITCMW owns and operates transmission assets only.

3. Does your company have a written policy regarding the treatment of customer data?

   a. Is the written policy regarding treatment of customer data shared with your customers?

   b. Does your process or policy include associated timeframes for notifying customers if a successful cybersecurity breach occurs that impacts customer data?

Response:

ITCMW does not receive or collect customer personally-identifiable information and, therefore, ITCMW does not have a policy regarding the treatment of customer data. ITC Holdings Corp. ("ITC"), on behalf of ITCMW, does have an Information Protection Program for dealing with Critical Infrastructure Protected Information. ITC also has a Business Code of Conduct. Collectively, these policies and program define how ITC protects data that is used for business purposes.

4. Please provide an organizational diagram of the company's security team, including all required support personnel

Response:

Please see diagram attached as Exhibit A.

5. Does the company have a qualified security team with adequate support personnel?

Response:

Please see response to Question 4.

6. Does your company participate in regional or national tabletop exercises, conferences, committees or other events related to critical infrastructure security threats and/or cybersecurity threats? If yes, please identify the various groups, activities or events.

Response:

ITCMW and/or ITC, on behalf of ITCMW, and its other operating companies, participates in the following regional and national tabletop exercises, conferences, committees, and other events related to critical infrastructure security threats and/or cybersecurity threats:

State of Michigan Annual Cybersecurity Exercise – Regional
State of Michigan Governor's Cyber Security Council - Regional
Michigan Critical Infrastructure Cybersecurity Forum - Regional
Michigan Public Service Commission Cyber Security Working Group - Regional
NERC GridEx (Cyber and Physical Security) Exercises – National

SPP Critical Infrastructure Protection Working Group - Regional
Public Service Commission Cyber and Physical Security forums - Regional
Department of Homeland Security conferences – National and Regional
Edison Electric Institute Cyber and Physical Security Group and conferences - National
North American Transmission Forum ("NATF") conferences and workshops- National
NATF Security Practices Group (Cyber and Physical) – National
American Society of Industrial Security - National
Secure World - National
Infragard - National
State conferences and outreach programs in all operating company regions - Regional
Peer reviews of physical security for other utilities - Regional

7. Does your company have an emergency preparedness plan (or plans) that include policies and procedures that include continuity of operations plans and disaster recovery plans related to critical infrastructure security threats? If yes,

a. Does your plan include alternative methods for meeting critical functions in the event of an incident?

b. Does your company have retainers or contracts for outside help in the event of an incident?

c. Does your company participate in any resource sharing agreements or mutual assistance agreements?

Response:

Yes. ITCMW has an emergency preparedness plan that includes continuity of operations and disaster recovery plans related to critical infrastructure protection for all threats.

a. Yes
b. Yes
c. Yes. ITCMW has mutual assistance agreements for power system restoration work support.

8. Does your company have an emergency preparedness plan (or plans) that include policies and procedures that include continuity of operations plans and disaster recovery plans related to cybersecurity threats?

a. Does your plan include alternative methods for meeting critical functions (continuity of operations plans and disaster recovery plans) in the event of an incident?

Response:

Yes. ITCMW has an emergency preparedness plan that includes continuity of operations and disaster recovery plans related to cybersecurity protection for all threats.

a. Yes.

9. Has your company conducted a physical and logical security evaluation of key assets in concert with federal guidelines?

Response:

Yes. ITCMW conducts a logical security assessment by a third party as described in Question 1 and also internally through its Cyber Vulnerability Assessment procedures which are conducted annually.

10. Has your company conducted a cybersecurity or physical security risk assessment?

Response:

Yes. ITCMW conducts both types of assessments during the third quarter of every year for CIP-defined substations.

11. Does your company have retainers or contracts for outside help in the event of an incident?

Response:

ITCMW does have contracts for outside help in the event of an incident. ITCMW, or ITC on behalf of ITCMW, maintains several contracts with cybersecurity and network equipment manufacturers as ongoing maintenance. These contracts include subject matter experts who can help ITCMW contain, mitigate, and eradicate cybersecurity threats.

12. Does your company participate in any resource sharing agreements or mutual assistance agreements?

Response:

Yes. ITCMW, or ITC on behalf of ITCMW, participates in the Midwest Mutual Assistance Group and the Great Lakes Mutual Assistance Group for system restoration. ITCMW, or ITC on behalf of ITCMW, also participates in several cybersecurity information resource sharing groups as part of its Cyber Intelligence program, including ES-ISAC, US-CERT, FBI Infragard, and several others.

13. Does your company have a process in place to alert of threats to critical infrastructures?

Response:

Yes. ITCMW has a Cyber Security Incident Response process which notifies ITCMW and ES-ISAC in the event to a cybersecurity event. As part of ongoing sharing of cyber threats,

ITCMW's Cyber Intelligence program is used to identify threats as described in Question 12 and disseminate the information to key stakeholders.

14. Does the company employ risk or vulnerability assessment tools that relate to critical infrastructure security or cybersecurity?

Response:

Yes. ITCMW has a comprehensive toolset to perform vulnerability assessments. These tools include threat and vulnerability scanning tools that identify targeted vulnerabilities based on the security configuration and patching level of a cyber asset against known exploits in the industry.

15. Does your company keep records of attempted or successful threats to critical infrastructure or cybersecurity?

Response:

Yes. ITCMW deploys Security Event and Incident Monitoring technologies designed with correlation to both identify and retain information regarding cybersecurity threats.

16. Does the company have a reporting process in the event of an attempted breach of critical infrastructure, whether successful or not?

Response:

Yes. ITCMW is required by NERC to report confirmed cybersecurity incidents to entities such as DOE and ES-ISAC. ITCMW may choose to communicate with other information sharing entities in the event of an attempted breach.

17. Does your company have an internal root cause analysis and correction action process to evaluate critical infrastructure security and to take action to prevent an event and/or recurrence?

Response:

ITCMW has an internal root cause analysis and correction action process, but it is not specific to critical infrastructure security. The current process is primarily geared towards bulk electric system reliability and security with focus on NERC Standards. ITCMW is in the process of developing a root cause analysis and correction action process specific to critical infrastructure security. However, all events are evaluated by subject matter experts and lessons learned are documented to include, as applicable, process improvement, corrective or preventive actions. Depending on the severity of the event, ITCMW management may request a root cause analysis and corrective action plan.

18. Does the company have a reporting process in the event of an attempted cybersecurity breach, whether successful or not?

Response:

Please see response to Question 16.

19. Does the company have a reporting process if a successful cybersecurity breach does occur that impacts customer data?

Response:

Please see response to Question 3.

20. Does your company have an internal root cause analysis and correction action process to evaluate cybersecurity and to take action to prevent an event and/or recurrence?

Response:

See response to Question 17.

21. What interaction/reporting, if any, should occur between your company and the Missouri Public Service Commission related to critical infrastructure security or cybersecurity?

Response:

ITCMW utilizes the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), operated by NERC on behalf of the Electricity Sector, and the Department of Energy's Electric Emergency Incident and Disturbance Report (OE-417), for the reporting of information related to critical infrastructure security or cybersecurity and believes that these processes are the best mechanism to provide this information to the Missouri Public Service Commission.

22. What format should be used to provide the interaction/reporting described in response to question 21?

Response:

Please see response to Question 21.

Respectfully submitted,

CURTIS, HEINZ,
GARRETT & O'KEEFE, P.C.

/s/ Carl J. Lumley

Carl J. Lumley, #32869
130 S. Bemiston, Suite 200
St. Louis, Missouri 63105
(314) 725-8788
(314) 725-8789 (FAX)
Email: clumley@chgolaw.com

Attorney for ITC Midwest, LLC

ITC Security Operations

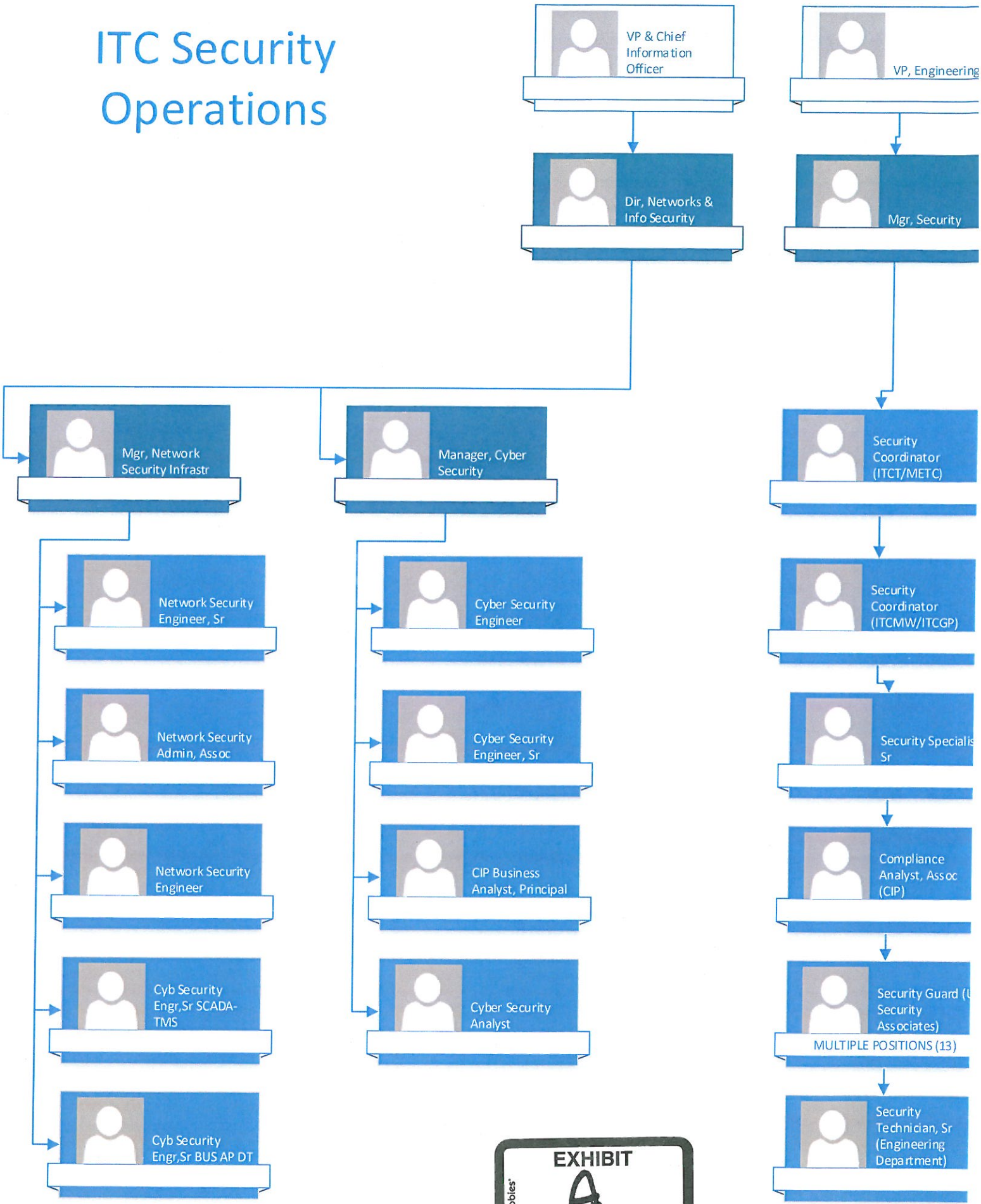

EXHIBIT
tabbies
A