BEFORE THE MISSOURI PUBLIC SERVICE COMMISSION

In the Matter of a Working Docket to Address	)	
Effective Cybersecurity Practices for Protecting	)	File No. EW-2013-0011
Essential Electric Utility Infrastructure	)	

ITC MIDWEST LLC'S RESPONSE TO THE COMMISSION'S JULY 17, 2012 ORDER DIRECTING A FILING

ITC Midwest LLC ("ITCMW"), for its Response to the Commission's July 17, 2012 Order Directing Notice and Directing Filing, submits as follows:

Background

1. On July 17, 2012 the Public Service Commission of the State of Missouri ("Commission") directed regulated electric utilities, including ITCMW, to answer 47 questions (some with subparts) regarding cybersecurity practices.

2. ITCMW's response ("Response"), set forth below, restates each question the Commission asked and then follows with ITCMW's response. Questions not applicable to ITCMW operations are noted as such.

Planning

1. Does your company have a cybersecurity policy, strategy or governing document?

Response: ITCMW has two documents that govern our cyber security posture and strategy.

- CIP-060 Information Security Policies: Defines policies implemented by ITCMW in order to protect the confidentiality and integrity of information stored and processed on ITCMWMW systems.

- CIP-065 CIP Cyber Security Policy: This document represents ITCMW's Cyber Security Policy and reflects ITCMW management's commitment and ability to secure ITCMW Critical Cyber Assets. This policy requires that ITCMW maintain an effective level of cyber security and provides a framework for compliance with North

American Electric Reliability Corporation (NERC) CIP standards CIP-002 through CIP-009 including provisions for emergency situations.

Copies of both documents are attached as Exhibits A and B.

2. Is the cybersecurity policy reviewed or audited? Internally or by an outside party? What qualifications does the company consider relevant to this type of review?

Response: ITCMW reviews its cyber security policies on an annual basis. ITCMW utilizes cyber security certified internal resources along with external vendor resources to perform these audits. Additionally, ITCMW's cyber security policies are audited by various regional authorities on a periodic basis.

In the selection of ITCMW's internal and/or external cyber security resources, ITCMW considers specific cyber security expertise and leading industry certifications as relevant qualifications. Two of the most prevalent industry certifications are the Certified Information Systems Security Professional (CISSP), and Certified Information Security Management (CISM) certifications.

3. Does your cybersecurity plan contain both cyber *and* physical security components, or does your physical security plan identify critical cyber assets?

Response: The cyber security plan does contain both cyber and physical security components. Additionally, there is a separate physical security plan in place. That document is titled SEC-002 Physical Security Plan. Our critical cyber assets are identified in a document titled CIP-541 Critical Asset and Cyber Asset List. Both of these documents are highly confidential and sensitive, and therefore are not attached to this filing.

4. Does your cybersecurity plan include recognition of critical facilities and/or cyber assets that are dependent upon IT or automated processing?

Response: The CIP-541 document referenced above recognizes critical facilities and cyber assets.

5. Are interdependent service providers (for example, fuel suppliers, telecommunications providers, meter data processors) included in risk assessments?

Response: ITCMW currently does not ask for vendor risk assessment, but is in the process of developing a process for including them.

6. Does your cybersecurity plan include alternative methods for meeting critical functional responsibilities in the absence of IT or communication technology?

Response: Yes.

7. Has your organization conducted a cyber risk or vulnerability assessment of its information systems, control systems and other networked systems?

Response: Yes. ITCMW is required to perform a complete Network Vulnerability Assessment on an annual basis under the NERC CIP standards. Moreover, the Cyber Security team performs regular vulnerability assessments periodically in addition to the annually scheduled assessment.

8. Has your company conducted a cybersecurity evaluation of key assets in concert with the National Cyber Security Division of the Department of Homeland Security? Has your company had contact with the National Cyber Security Division of DHS or other elements of DHS that may be helpful in this arena?

Response: No, ITCMW has not conducted a cyber security evaluation of key assets in concert with the National Cyber Security Division of the Department of Homeland Security ("DHS"). ITCMW has, however, worked with the National Cyber Security Division of DHS, and DHS has participated in ITCMW's Cyber Security Advisory Group and presented to ITCMW's IT Department.

9. Has your cybersecurity plan been reviewed in the last year and updated as needed?

Response: Yes. The security plan is required to be reviewed annually under the NERC CIP requirements and is updated as needed.

10. Is your cybersecurity plan tested regularly? Is it tested internally or by or with a third party?

Response: All components of ITCMW's cyber security plan are reviewed and updated on a regular basis. ITCMW performs an annual test of its cyber security incidence response plan in accordance with existing policy. This plan is tested with outside vendor participation. A copy of the applicable policy (CIP-068 – Incident Response Plan) is attached as Exhibit C.

11. What is your process/plan for managing risk?

Response: ITCMW currently has a vulnerability management program in place to continuously assess and address risk. Please see the response to Question 30 for more details on personnel risk assessments.

12. Has your company undergone a whole-system, comprehensive cybersecurity audit or assessment? When and by whom?

Response: Yes. A complete NERC CIP audit was conducted in 2011. The audit was performed by the appropriate NERC regional compliance entities, RFC, MRO and SPP.

Standards

13. Describe the company's compliance status with NERC CIP-002 through CIP009.

Response: ITCMW has a NERC CIP compliance program in place and is continuously monitoring compliance and improving program components.

14. What collaborative organizations or efforts has your company interacted with or become involved with to improve its cybersecurity posture (such as NESCO, NESCOR, Fusion centers, Infragard, US-CERT, ICS-CERT, ES-ISAC, SANS, the Cross-Sector Cyber Security Working Group of the National Sector Partnership, etc.)?

Response: ITCMW has interacted with or been involved with Infragard, US-CERT and ES-ISAC.

15. Can your company identify any other mandatory cybersecurity standards that apply to its systems? What is your company's plan for certifying its compliance or identifying that it has a timetable for compliance?

Response: At present, the only mandated cyber security standards that apply to ITCMW are the NERC CIP standards. NERC maintains a schedule for audits under which ITCMW will be audited every three years. At the same time, there is a once-a-year Reliability Standard Audit (Self Certification) which ITCMW is required to submit to the regional reliability entities (MRO, RFC and SPP).

16. Compliance as a floor, not a ceiling: are there beyond-compliance activities? Given that there are very little or no cybersecurity standards specified at this point by State regulatory authorities in regard to the distribution portion of the electrical grid, what are you doing to get in front of this?

Response: ITCMW goes beyond minimal compliance levels in several areas. Two examples of this are with regard to the Network Vulnerability Assessments (NVA) and ITCMW's annual cyber security awareness training. Compliance standards require only an annual NVA, but ITCMW performs regular NVA's on a weekly basis. The cyber security awareness training is officially only a requirement for those personnel with access to critical assets and critical cyber assets. ITCMW requires that all internal and external resources complete this training annually.

Since ITCMW only owns, operates and maintains transmission facilities, the second part of this question is not relevant to it.

17. How do you determine which systems, components and functions get priority in regard to implementation of new cybersecurity measures?

Response: Assets identified as "Critical" under the NERC CIP standards (both cyber and non-cyber assets) are given the highest priority.

18. Is cybersecurity addressed differently for each major electrical component: distribution, transmission, generation, retail customers?

Response: ITCMW only owns, operates and maintains transmission facilities. ITCMW does not have any distribution or generation assets or responsibilities.

Procurement Practices

19. Has your organization conducted an evaluation of the cybersecurity risks for major systems at each stage of the system deployment lifecycle? What has been done with the results?

Response: ITCMW performs an internal risk assessment when deploying major systems as part of the Project Management Office. New systems are put through a cyber security review prior to being approved. The results of any assessments that are conducted are evaluated internally.

20. Are cybersecurity criteria used for vendor and device selection?

Response: ITCMW currently does not have or use cybersecurity criteria for vendor and device selection, but is in the process of developing such criteria as part of the vendor risk assessment.

21. Have vendors documented and independently verified their cybersecurity controls? Who is the verifier and how are they qualified?

Response: ITCMW currently does not ask for these controls from its vendors, but ITCMW plans to add those requirements as part of the vendor risk assessment that is being developed currently.

22. Does your organization perform vulnerability assessment activities as part of the acquisition cycle for products in each of the following areas: cybersecurity, SCADA, smart grid, internet connectivity and Web site hosting?

Response: The various internal teams responsible for the types of devices and services listed in this question do perform a cybersecurity assessment before the implementation or upgrade of a device and prior to deployment of any new service. We utilize various methods for the assessments, including automated scanning tools, cybersecurity checklists or other manual processes as required. The results of these assessments are stored in our change/configuration management system.

23. Has the company managed cybersecurity in the replacement and upgrade cycle of its networked equipment? Does this include smart meters?

Response: Yes. The various teams responsible for replacing and/or upgrading networking equipment perform a cyber security assessment before replacing or upgrading

any device. The cyber security measures include the use of automated scanning tools, cyber security checklists and any other manual processes deemed appropriate. The assessment data is stored within the ITCMW change/configuration management system.

Since ITCMW only owns, operates and maintains transmission facilities, ITCMW does not own any smart meters.

24. What kind of guidance do you follow to ensure that your procurement language is both specific and comprehensive enough to result in acquiring secure components and systems? (Note: Does your company include Cyber Security Procurement Language for Control Systems within its Procurement Language? Available at http://www.us-cert.gov/control systems/pdf/FINAL-Procurement Language Rev4 100809.pdf IEC 62443).

Response: As a NERC registered entity within the MRO regional entity, ITCMW Midwest largely relies upon the CIP rules promulgated by NERC and upon the company's subject-matter experts for guidance in the procurement and acquisition of secure control system components and systems. ITCMW Midwest also engages in a bidding process that evaluates the vendors based on their competency within the areas of security and reliability for control systems which results in contracts and scopes of work that cover the necessary areas of CIP compliance, security and reliability. ITCMW Midwest does not, however, specifically rely upon or include the Homeland Security's Cyber Security Procurement Language for Control Systems within its procurement language.

25. Would the company be willing to provide a presentation to the Commission (as a closed, *in-camera* and non-disclosable setting with no documentation or materials coming into possession of the PUC)?

Response: Yes.

Personnel and Policies

26. Is cybersecurity budgeted for? What is the current budget for cybersecurity activities relative to the overall security spending?

Response: Yes, ITCMW annually budgets for cyber security. The 2012 budget for cyber security is approximately $300,000. The 2012 budget for overall security spending is approximately $1,500,000.

27. Are individuals specifically assigned cybersecurity responsibility? Do you have a Chief Security Officer and do they have explicit cybersecurity responsibilities?

Response: ITCMW does have individuals with assigned cyber security responsibility. We do not currently have a Chief Security Officer. The ITCMW Chief Information Officer (CIO) serves as the NERC CIP Sr. Manager Designate. The Director of IT Services is responsible for the cyber security program.

28. Does your company employ IT personnel directly, use outsourcing or employ both approaches to address IT issues? For companies that lack a full IT department, explain if one individual in your company is held responsible for IT security

Response: ITCMW utilizes both employees and contractors to manage IT issues. The Director of IT Services is responsible for IT security at ITCMW.

29. What training is provided to personnel that are involved with cybersecurity control, implementation and policies?

Response: ITCMW provides annual Cyber Security Awareness training as required by the NERC CIP Standards and Individualized training for employees and contractors on an as needed basis.

30. What personnel surety/background checking is performed for those with access to key cyber components? Are vendors and other third parties that have access to key cyber systems screened?

Response: A comprehensive background check is performed on all personnel, including company employees, vendor representatives and any third parties prior to the granting of access to cyber assets and critical cyber assets. In accordance with the NERC reliability standards pertaining to critical infrastructure protection, ITCMW is required to have a "documented personnel risk assessment program" for personnel having authorized cyber access or authorized unescorted physical access to critical cyber assets.

31. For the most critical systems, are multiple operators required to implement changes that risk consequential events? Is a Change Management process in place, especially in regard to systems which could present a risk to electrical reliability?

Response: Yes, multiple operators are required to implement changes that risk consequential events. This requirement is contained in ITCMW's internal policy, CIP-055 – Change Control and Configuration Management Process, a copy of which is attached as Exhibit D.

32. Has business process cybersecurity has been included in continuity of operations plans for areas like customer data, billing, etc.?

Response: No, since ITCMW only owns, operates and maintains transmission facilities, ITCMW has no customer billing system. All transmission billing is administered by the relevant Regional Transmission Organization (RTO) on behalf of ITCMW.

33. Describe the company's current practices that are employed to protect proprietary information and customer privacy and personal information. Does the company have an information classification and handling policy?

Response: ITCMW employs a classification policy for information deemed critical under the NERC CIP Standards. The policy is titled CIP-018 Critical Cyber Asset Information Classification, and it defines the identification, classification, protection, and handling of information associated with critical cyber assets in electronic format, as well as additional controls regarding the secure handling of hard copy information. A copy of the policy is attached as Exhibit E.

34. Does the company collect personally identifiable information electronically? What type of information (name, address, social security number etc.) is collected? Is there a policy for the protection of this information? How is your company ensuring that any third parties you deal with are also keeping this information secure?

Response: No.

35. Identify whether the company has identified points of contact for cybersecurity:

a. Emergency management/law enforcement?

Response: No for cybersecurity. Yes for physical security

b. National security? DHS, including protective and cybersecurity advisors?

Response: No for cybersecurity. Yes for physical security

c. Fellow utilities, ISOIRTO, NERC, CIPC, others?

Response: No for cybersecurity. Yes for Operations.

d. NESCO, VirtualUSA, Einstein, Fusion centers, Infragard, USCERT, ICS-CERT, ES-ISAC?

Response: No for cybersecurity. Yes for Operations.

e. Interdependent system service providers?

Response: No

Systems and Operations

36. Is cybersecurity integrated between business systems and control systems? For the existing grid and for the smart grid?

Response: Yes, ITCMW operates multiple DMZ networks which are separated by firewalls and which require multi-factor identification to access control system resources for the existing electric transmission grid.

A DMZ (sometimes referred to as perimeter networking) is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

37. Have logical and physical connections to key systems been evaluated and addressed?

Response: Yes, the logical and physical connections to key systems have been evaluated and documented. All unused connections and switchports are disabled. The physical and logical connections are visually inspected at least annually and documentation is updated accordingly.

38. Does the company maintain standards and expectations for downtime during the upgrade and replacement cycle?

Response: Yes. We have redundant systems in place which interface with the electric transmission system so ITCMW is able to perform upgrades or replacements to systems in the main "hot" site while operations are continuing to run in the failover site. We can then transfer operations back to the primary site for testing prior to failing back.

39. Does the company have equipment dependent on remote upgrades to firmware or software, or have plans to implement such systems? Does the company have a plan in place to maintain system cybersecurity during statistically probable upgrade failures? Is there a schedule for required password updates from default vendor or manufacturer passwords?

Response: Yes, ITCMW has equipment dependent on remote upgrades to firmware or software. ITCMW also has a failover hot site that it can switch operations to if there is a primary site issue. This is addressed in ITCMW Policy CIP-055 - Change Control and Configuration Management Process, a copy of which is attached as Exhibit D.

Likewise, ITCMW maintains a required schedule for password updates as written in ITCMW's Policy CIP-024- Password Standards, a copy of which is attached as Exhibit F.

40. Has cybersecurity been identified in the physical security plans for the assets, reflecting planning for a blended cyber/physical attack?

Response: No.

41. Discuss what the PUC can do to assist your company in the area of cybersecurity.

Response: ITCMW is not aware of any additional assistance the PUC could provide at this time.

42. What network protocols (IP, proprietary, etc.) are used in remote communications? Is the potential vulnerability of each protocol considered in deployment?

Response: ITCMW utilizes HTTP, HTTPS, FTP & SFTP as remote communications protocols from the Internet to the secure DMZ environment discussed above. All other protocols utilized for remote communications are encrypted within a VPN tunnel utilizing at least 168 bit encryption prior to being sent over both public and our private networks.

As part of ITCMW's Project Management Office policy, all new applications and/or protocols must go through a security assessment and approval prior to deployment. ITCMW is also actively seeking opportunities to retire older, less secure protocols from our environment.

43. Does the company have a log monitoring capability with analytics and alerting- also known as "continuous monitoring"?

Response: Yes. ITCMW uses a product called Qradar to capture logs from defined systems and that product provides alerts that inform the IT Support team of any issues.

44. Are records kept of cybersecurity access to key systems?

Response: Yes, using the Qradar system. These logs are retained for a minimum of 6 months.

45. Are systems audited to detect cybersecurity intrusions?

Response: Yes. ITCMW uses Qradar to inform it of intrusions or attempted intrusions.

46. Are records kept of successful cybersecurity intrusions?

Response: Yes, if there is an intrusion the system will retain the logs and ITCMW would archive such logs for at least three years.

47. What reporting occurs in the event of an attempted cybersecurity breach, successful or not? To whom is this report provided (internal and external)? What reporting is required and what is courtesy reporting?

Response: Cyber security breaches that impact, or that could potentially impact, the Bulk Electric System (BES) are required to be formally reported to the Electronic Sector - Information Sharing and Analysis Center (ES-ISAC). Additionally, internal reports are provided to key stakeholders and executive management.

Respectfully submitted,

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

/s/ Carl J. Lumley

Carl J. Lumley, #32869
130 S. Bemiston, Suite 200
Clayton, Missouri 63105
(314) 725-8788
(314) 725-8789 (Fax)
clumley@lawfirmemail.com

Attorneys for ITC Midwest, LLC

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing was emailed, faxed or mailed by U.S. Mail, postage paid, this 31st day of August, 2012, to the persons shown on the attached list.

/s/ Carl J. Lumley

General Counsel's Office
Missouri Public Service Commission
200 Madison Street, Suite 800
P.O.Box 360
Jefferson City, MO 65102
gencounsel@psc.mo.gov

Lewis Mills
Office of the Public Counsel
200 Madison Street, Suite 650
P.O. Box 2230
Jefferson City, MO 65102
opcservice@ded.mo.gov