BEFORE THE PUBLIC SERVICE COMMISSION OF THE STATE OF MISSOURI

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

ORDER DIRECTING NOTICE AND DIRECTING FILING

Issue Date: July 17, 2012 Effective Date: July 17, 2012

Utility systems have become more and more complex with the advancement of technology and perhaps no utility industry has become more technologically linked than the electric industry. The electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure as part of nationwide efforts - commonly referred to as the "smart grid," which is aimed at improving reliability and efficiency and facilitating the use of alternative energy sources such as wind and solar.

Smart grid technologies include metering infrastructure ("smart meters") that enable two-way communication between customers and electricity utilities, smart components that provide system operators with detailed data on the conditions of transmission and distribution systems, and advanced methods for controlling equipment. The use of these systems can bring a number of benefits, such as fewer and shorter outages, demand-side conservation and lower electricity rates. However, increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities, which can be exploited by attackers.

Cybersecurity of this interconnected system involves not only the physical distribution and transmission grids, substations and offices, but also equipment and

systems that communicate, store and act on data. Cybersecurity encompasses not only utility-owned systems, but aspects of customer and third-party components that interact with the grid, such as the advanced meters. And more than simply being a function of hardware, cybersecurity is critically important as a function of software, data and the networks that use data to keep the system operating.

Cybersecurity vulnerabilities exist wherever computer systems and data exist. With the advent of smart grid technologies, which layer software on top of utility operations and computer systems, threats become increasingly likely and relevant. The aims and implications of cybersecurity violations vary widely. Gaining system control, the ability to remotely modify and operate the system as a vehicle for attack, is but one threat. Data theft, or "exfiltration," is also a known and on-going problem. Cybersecurity must also protect against inadvertent sources, such as user errors, hardware failure, software bugs, operator errors or just plain negligence. Natural disasters can also present a major threat.

The Commission finds itself at a critical juncture for infrastructure protection as the grid transitions from a previously isolated environment to a complexly interconnected one. With such a dynamic and broad landscape to consider, cybersecurity cannot be a stagnant prescription. It should evolve as technology, threats and vulnerabilities evolve, introducing the building blocks that stand the test of time while still being flexible enough to meet changing cybersecurity requirements.

The Commission is charged with the duty of assuring that public utility companies provide safe and adequate service at just and reasonable rates. Because cybersecurity threats challenge the reliability, resiliency and safety of the electric grid, and because

utility spending to address cyber vulnerabilities can impact the bills that customers pay, the Commission must explore, and ensure, the integrity of the electric utilities' internal cybersecurity practices. It is with this goal in mind that the Commission has opened this working docket, and as part of its initial investigation, the Commission will direct its regulated electric utilities to answer the following questions:

Planning

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

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?

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

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

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

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

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

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?

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

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

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

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

Standards

13. Describe the company's compliance status with NERC CIP-002 through CIP-009.

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.)?

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?

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?

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

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

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?

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

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

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?

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

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)?

Personnel and Policies

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

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

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.

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

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?

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?

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

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?

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?

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

a. Emergency management/law enforcement?

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

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

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

e. Interdependent system service providers?

Systems and Operations

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

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

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

39. Does the company have equipment dependant 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?

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

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

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

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

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

45. Are systems audited to detect cybersecurity intrusions?

46. Are records kept of successful cybersecurity intrusions?

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?

Once this initial step is completed, the Commission will determine how it wishes to proceed. This docket may involve future workshops, on-the-record presentations, rulemaking, or taking individual measures in general rate-making proceedings.

THE COMMISSION ORDERS THAT:

1. The Commission's Data Center shall serve a copy of this order upon all Missouri regulated electric utilities. The Data Center shall add those utilities to the certified service list.

2. The Commission's Data Center shall serve a copy of this order upon the county commission, or other equivalent governmental entity, of each county within the service areas of all Missouri regulated electric utilities.

3. The Commission's Public Information Office shall make notice of this order available to the members of the General Assembly representing the service areas of all Missouri regulated electric utilities and to the news media serving the service areas of all Missouri regulated electric utilities.

4. No later than August 31, 2012, all Missouri regulated electric utilities shall file answers to all of the questions delineated in the body of this order.

5. This order shall become effective immediately upon issuance.

BY THE COMMISSION

Steven C. Reed
Secretary

(S E A L)

Harold Stearley, Deputy Chief Regulatory Law Judge, by delegation of authority pursuant to Section 386.240, RSMo 2000.

Dated at Jefferson City, Missouri,
on this 17th day of July, 2012.