

**BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI**

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

EMPIRE'S RESPONSE TO ORDER DIRECTING FILING

COMES NOW The Empire District Electric Company ("Empire") and, in response to the Missouri Public Service Commission's (the "Commission") Order Directing Notice and Directing Filing issued on July 17, 2012, respectfully state as follows:

Planning

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

Response – Yes

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 – Yes, Empire’s cyber security policy is reviewed and audited both internally and externally. Audits are performed by appropriate regulatory agencies and external auditors qualified to review policies and procedures.

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

Response – Yes

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

Response – Yes

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

Response – Yes

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

Response – Our cyber security plan does not, however Empire’s other emergency plans take these contingencies into account.

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

Response – Yes

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 – We have not performed a cybersecurity evaluation directly with the National Cyber Security Division of the DHS. However, Empire has performed an evaluation with NERC who has direction and privileged information from the DHS.

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

Response – Yes

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

Response - Yes. Internally.

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

Response – Empire’s risk methodology standard is based on NERC standard CIP-002-3.

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

Response – Yes. SPP in 2009.

Standards

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

Response - Empire complies with 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.)?

Response - Empire has reported to and included ES-ISAC in cyber security response drills.

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 - Empire uses established NERC cyber security standards for its governing standards. Empire uses NERC's compliance timeline for its program.

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 – Empire complies with the NERC standards. Going beyond NERC standards can create NERC compliance issues, and any additional cost required to go beyond NERC standards creates additional issues.

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

Response - Empire follows CIP-002-3, as well as NERC's guidance of new measures that are developed in the NERC standards drafting process.

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

Response - No

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 - Yes. Future systems are reviewed with cybersecurity risks in the forefront of the evaluation.

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

Response – Yes

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

Response - Yes. Both the vendor and/or Empire can document and verify qualifications independently.

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 - Yes

SCADA – YES

Smart Grid – N/A

Internet Connectivity – NO

Web Site Hosting - YES

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

**Response – Upgrade cycle of networked equipment – Yes
Smart Meters – N/A**

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](http://www.us-cert.gov/control%20systems/pdf/FINAL-Procurement%20Language%20Rev4%20100809.pdf) IEC 62443).

Response – The company has internal procedures and policy for guidance.

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, depending on the timing of the presentation, and the timing of Empire's next SPP/NERC audit.

Personnel and Policies

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

Response – Yes. Budgets for cybersecurity are proprietary.

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

Response – Yes to all

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 – 1. Yes, 2. Yes, 3. N/A

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

Response – Empire complies with NERC standard CIP-004-3.

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 – 1. Empire complies with CIP-004-3. 2. Empire complies with CIP-004-3 and CIP-006-3

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 – Empire follows the protocols in CIP-007-3 and CIP-005-3 for change management.

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

Response – Yes

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 – Empire restricts access to this information and requires a court order to release customer information.
Yes**

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 – 1. Yes, 2. Yes, 3. Yes, 4. Contracts

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, USCERT, ICS-CERT, ES-ISAC?
- e. Interdependent system service providers?

Response – A. Yes, B. Yes, C. Yes, D. Yes, E. Yes.

Systems and Operations

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

Response – Yes

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

Response – Yes

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

Response – Yes

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?

Response – 1. Yes, 2. Yes, 3. Yes

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

Response – Yes see NERC standard CIP-006-3

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

Response – The PUC can help ensure that another layer of regulation is not added to this area

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

Response – 1. Empire considers its network protocols to be proprietary. 2. Yes

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

Response – Yes

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

Response – Yes

45. Are systems audited to detect cybersecurity intrusions?

Response – Yes

46. Are records kept of successful cybersecurity intrusions?

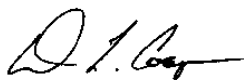
Response – Yes

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 – Reporting occurs in accordance with NERC standard CIP-008-3 and The Department of Energy form OE-417.

WHEREFORE, Empire respectfully requests that the Commission consider this response to comply with the Commission's Order Directing Notice and Directing Filing.

Respectfully Submitted,



Dean L. Cooper #36592
Brydon, Swearngen & England P.C.
312 East Capitol Avenue

P.O. Box 456
Jefferson City, MO 65102-0456
Telephone: 573-635-7166
Facsimile: 573-636-6450
E-mail: dcooper@brydonlaw.com

**ATTORNEYS FOR THE EMPIRE
DISTRICT ELECTRIC COMPANY**

CERTIFICATE OF SERVICE

The undersigned certifies that a true and correct copy of the foregoing document was sent by electronic mail, on August 24, 2012, to the following:

Kevin Thompson
Office of the General Counsel
Governor Office Building, 8th Floor
Jefferson City, Mo 65101
Kevin.thompson@psc.mo.gov

Lewis Mills
Office of the Public Counsel
Governor Office Building, 6th Floor
Jefferson City, MO 65101
lewis.mills@ded.mo.gov

