Critical Infrastructure Protection Supply Chain Risk Management

Written Comments of Maria Jenks

Kansas City Power & Light Company

Chairman Bay, commissioners, staff, and fellow panelists, I am Maria Jenks, Vice President—Supply Chain, Kansas City Power & Light Company, also known as KCP&L. Today, I am here representing KCP&L, which appreciates the Commission's continued strong interest in critical infrastructure protection supply chain risk management issues, and welcomes the opportunity to participate in today's technical conference.

The CIP version 5 requirements provide the right approach in mandating the "what" but not the "how" in terms of cyber security and supply chain risk management. KCP&L uses existing cyber security and supply chain risk management guidelines and practices to help determine the "how" for regulatory compliance as well as enterprise-wide risk management. We do not believe a new or modified FERC-mandated standard is needed to address supply chain cybersecurity risks for industrial control system hardware, software, and computing and networking services associated bulk electric system operations.

Long held fundamental goals for every utility supply chain, whether acquiring turbines, transformers, or cyber assets, is ensuring security and having confidence in the quality of the purchased product or service. In light of these fundamental goals it is simply a good business practice to promote supply chain security. The company has every incentive to safeguard KCP&L's operational integrity by identifying and mitigating supply chain risks.

My comments will summarize KCP&L's current supply chain risk management efforts, which are representative of existing utility procurement practices and industry supply chain

initiatives regarding information and communications technology and hardware, software, and services in other critical infrastructure sectors.

Mitigating Supply Chain Cybersecurity Risk

KCP&L manages supply chain risk through a collaborative approach with internal stakeholders and suppliers; using widely-accepted risk-based frameworks and processes to assess, manage and monitor critical risk areas. KCP&L employs an enterprise risk management framework, based upon COSO[1], to assess enterprise risk, including but not limited to cyber and physical security, reliability, operational, and supply chain risks. Enterprise risk mitigation strategies are deployed and monitored. The process is coordinated by KCP&L's internal Risk Management department, engaging leaders of all business units across the company. There is added monitoring by Risk Management, Internal Audit, Corporate Compliance, FERC Compliance, with assurance through controls and quality control procedures within business operating units. Basically, the enterprise risk process is organic and foundational throughout the organization, including the supply chain function.

Initial Assessments and Risk Profiles

Supply Chain processes and procedures require completion of supply chain risk assessments; cyber and physical security risk is a dimension in the assessments and always considered. A supplier risk assessment framework is used to identify and assess suppliers that

[1] COSO: The Committee of Sponsoring Organizations of the Treadway Commission issued an Enterprise Risk Management - Integrated Framework model that is widely used. "The framework describes the critical principles and components of an effective enterprise risk management process, setting forth how all important risks should be identified, assessed, responded to and controlled. It also provides a common language. …[It] sets forth how a company applies enterprise risk management in its strategic planning and also describes techniques some companies are using in identifying and managing risk… The framework also describes roles of key players in the enterprise risk management process." Executive Summary-FAQs, *COSO Enterprise Risk Management-Integrated Framework* (September 2004)

pose a particular risk or threat to operations. Additionally, Supply Chain assesses risk at the front-end of the process for major procurements of goods or services.

While processes and procedures require cybersecurity, physical security and reliability risk assessments, they are only a component of the broader range of business risks evaluated and mitigated by Supply Chain.

Technical Experts' Review

Once a procurement project is initiated, purchasing procedures require Supply Chain work with relevant technical experts, often involving engineering and project managers—leveraging their expertise in establishing technical specifications included in Requests for Proposals ("RFP").

The RFP provides detailed design and material specifications as well as other technical requirements and standards. The RFP technical specifications help guide discussions with prospective suppliers and are critical to a robust evaluation process, including identified cyber and physical security risks. Risk assessments also guide decisions as to contracting approaches and structures.

DOE and DHS Endorsed Cybersecurity Procurement Language

KCP&L utilizes the Cybersecurity Procurement Language for Energy Delivery Systems (CPLEDS)[2]. CPLEDS was endorsed and is promoted by Department of Energy ("DOE") and Department of Homeland Security ("DHS") as part of their cybersecurity initiatives. KCP&L

[2] *Cybersecurity Procurement Language for Energy Delivery Systems*, April 2014, published by the Energy Sector Control Systems Working Group (ESCSWG), a public-private partnership consisting of energy delivery systems cybersecurity experts from government and industry that support the Electricity Sub-sector Coordination Council, Oil and Natural Gas Sector Coordinating Council, and the Government Coordinating Council for Energy under the Critical Infrastructure Partnership Advisory Council framework. ESCSWG was formed in 2007.

developed a guideline based on CPLEDS procurement language to assess risk relating to hardware, software, and communication type purchases. Using the CPLEDS inspired guideline, appropriate contract provisions are incorporated into procurement agreements.

Supplier Evaluation and Approval

KCP&L employs a rigorous supplier evaluation, qualification and approval process. Due diligence includes items such as safety record, financial and credit standing, security standards and certifications, and other quality and security checks depending on the nature of work and supplier. KCP&L works extensively with suppliers to gain understanding of their manufacturing processes, subcontracting plans, supply chain, and other relevant information to the procurement transaction. Site visits and inspections are employed when appropriate. KCP&L also identifies if data will be shared; whether the supplier will have access to company systems or data; whether suppliers' systems will interface with KCP&L's systems; whether any of the suppliers' components have an electronic component or wireless transmittal of data capability; or whether any other privileged financial or commercial information will be shared.

KCP&L further assesses supplier and cyber asset risk based upon threat intelligence received from sources such as the Federal Bureau of Investigation ("FBI"), DHS, Electricity Information Sharing and Analysis Center ("E-ISAC"), and other utilities.

Subject Matter Expert Review and Mitigation

KCP&L employs a rigorous, formal internal review and approval process for each procurement before a contract is signed, including Subject Matter Experts ("SME") from Risk Management, Information Security, Information Technology, Corporate Security, Engineering,

Operations, Warranty, Legal, Compliance, or other affected stakeholders, that review pertinent sections of contracts prior to execution. Cybersecurity affected procurements have SME for each technical area as well. Controls and protocols are in place to help ensure that the risks identified during the assessment process have an appropriate written mitigation plan with documentation and confirmation of completion.

After Contract Execution

After a contract is executed, there are a number of monitoring activities that occur. Depending on the identified risk level established during the initial and continuing risk assessment, and based on the nature of the project, KCP&L may require: overseeing the manufacturing process; detailed receipt and inspection procedures; quality control; testing; independent third-party audits or reviews; physical and cybersecurity measures; scanning for vulnerabilities; and other monitoring and control activities required to ensure the security of the asset. Contract management processes are used to confirm and document execution of elements of the contract, including security related provisions.

Continuing Supplier Assessment

KCP&L works with key suppliers to develop scorecards that include metrics to regularly track and monitor service level agreements, quality, and deliverables. Regular business review meetings are held to report on results and drive reliability, effectiveness, and accountability. KCP&L's change order control process, and other contract management processes, work to ensure that safety plans, security audits, and quality certifications are available and up to date.

Ultimately, KCP&L believes setting the right tone and expectations with suppliers is a critical component of its supply chain risk management strategy.

In closing, KCP&L supports Edison Electric Institute's ("EEI") work on Principles and Resources and Recommendations for Managing Supply Chain Cybersecurity Risk. We believe industry participants responsible for the reliable operation of the BES will adopt the guidelines and build a system of risk management and controls in accordance with the guidelines. In the event there is a need to amend the guidelines, we support the proposition that the industry would need extensive engagement with stakeholders (entities and suppliers) as part of that initiative. Because of the complexity of systems and sensitive issue areas, we support EEI's contention that NERC CIP regulations have the right approach in mandating the "what" but not the "how" in terms of supply chain risk management. We would offer the "how" is suggested in the available guidelines and CPLEDS as a starting point for voluntary discussions with industry participants to incorporate concepts versus prescriptive requirements. The DOE and DHS endorsed CPLEDS has already advanced supply chain security initiatives. Both support the active and continuing work to strengthen supply chain cybersecurity.