ACEC
American Council of Engineering Companies
100 Years of Excellence

David A. Raymond
President & CEO

June 16, 2016

Norman C. Bay, Chairman
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

RE: Reliability Standards for Critical Infrastructure Protection and Supply Chain Management, FERC Docket No. RM15-14-000

Dear Chairman Bay:

On behalf of the American Council of Engineering Companies (ACEC) – the business association of the nation's engineering industry – I want to convey the industry's perspectives and concerns over the potential development of a new cybersecurity supply chain rule by the Federal Energy Regulatory Commission (FERC).

ACEC members firms, numbering more than 5,000 firms representing over 500,000 employees throughout the country, are engaged in a wide range of engineering works that propel the nation's economy, and enhance and safeguard America's quality of life. Council members are actively involved in every aspect of the energy marketplace.

Supply chain cybersecurity is of growing concern to all our members. ACEC opposes a potential future FERC supply chain ruling that could create insupportable burdens on engineering firms and our utility clients. While we believe that present cybersecurity controls and voluntary practices are highly effective, input by engineering service providers would assist FERC in producing a more effective approach in minimizing the impacts on competition, risk allocation, and pricing.

FERC's originally proposed supply chain rule – which was withdrawn earlier this year in the face of industry opposition – cited model Department of Energy (DOE) supply chain procurement language for energy delivery systems. ACEC members report that the DOE guidance has been voluntarily used in negotiations on agreements in the electricity utility sector for procurement of professional engineering services. In formal comments on the originally proposed rule, the utility industry also indicated it uses the DOE guidance language and could support further guidance development. While ACEC has concerns with the DOE model language, we see its further development and clarification as a potentially constructive direction, if continued on a wholly voluntary, rather than a mandatory basis.

That said, the Council is concerned that FERC may take DOE's voluntary procurement guidance and make it mandatory in a future supply chain rule. If misapplied as mandatory policy, the

T 202-347-7474 F 202-898-0068 draymond@acec.org
1015 15th Street, NW, 8th Floor Washington, DC 20005-2605 www.acec.org

DOE procurement language would impose unrealistic obligations, standards of care, and potential liability on professional services related to the supply chain. As a consequence, services currently provided by engineering firms may be uninsurable under current professional liability insurance policies. Other industries supporting the supply chain have raised similar concerns, noting that the effect of FERC's approach will be to stifle competition, impair innovation, and increase costs.

Specifically, the DOE guidance language includes "integrator" requirements that impose responsibilities on engineering firms and other supply chain elements for control of software development; personnel management systems; industrial system controls (SCADA); and long-term or post-contract reporting/remediation requirements (vulnerability testing and mitigation). Engineering firms do not typically develop such software and hardware, yet the guidance language suggests they should assume such liability for their use. They also do not monitor and report vulnerabilities for the software and hardware. This "one-size-fits-all" approach amounts to a significant reallocation of risk, imposing liability on engineering firms that they can neither manage, nor price. The result will be fewer firms willing to perform services for this industry. The requirements should be scaled to the scope and responsibilities of the parties involved in the supply chain.

Finally, ACEC opposes the potential future FERC ruling for reasons cited by many owners, operators and vendors in the electricity sector. There is no "reliability gap" that needs to be filled. Current voluntary risk management frameworks are effective. Since regulation cannot keep up with changes in cybersecurity, the potential future ruling is impractical.

FERC needs to proceed with care in this area, as the same industrial control systems are widely used across infrastructure sectors beyond energy. FERC's actions could become the basis of a broader standard of care, impacting a wide array of industry stakeholders with the unintended consequences of diminishing competition, creating a chilling effect on innovation, and increasing costs.

In short, ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this rulemaking. We fully appreciate the concerns over how risk can be adequately managed under any future proposed ruling. Our member firms' reputations depend upon professional performance and innovation in an atmosphere of collaboration. However, we are concerned that a supply chain ruling based on the DOE guidance language will not support, and may actually impair, broad-based cost-effective infrastructure reliability.

Sincerely,

David A. Raymond
President and CEO

cc: Commissioner Cheryl A. LeFleur
Commissioner Tony Clark
Commissioner Colette D. Honorable
Michael Bardee (Director, Office of Electric Reliability) michael.bardee@ferc.gov
Dr. David Ortiz (Deputy Director, Office of Electric Reliability) david.ortiz@ferc.gov
Cynthia Pointer (Division Director of Reliability Standards & Security, Office of Electric Reliability) cynthia.pointer@ferc.gov
Rhonda Dunfee (Manager, Division of Reliability Standards & Security, Office of Electric Reliability) Rhonda.dunfee@ferc.gov
Dan Phillips (Energy Industry Analyst) Daniel.Phillips@ferc.gov