NIST Cybersecurity Framework Comments December 13, 2013

MidAmerican Energy Holdings Company appreciates the opportunity to provide comments on the National Institute of Standards and Technology (NIST) development of a Cybersecurity Framework defined in Executive Order 13636, *Improving Critical Infrastructure Cybersecurity.*

Comments

MidAmerican Energy Holdings Company has been engaged in closely following the Critical Infrastructure Cybersecurity Executive Order and subsequent Cybersecurity Framework development led by NIST. Through careful review of the draft documents and ongoing engagement with similarly-situated industry partners, our comments support the general consensus among industry partners, including specific comments developed by the Edison Electric Institute and American Gas Association.

As a public utility operating in multiple critical infrastructure sectors in multiple U.S. states, we believe the Cybersecurity Framework is a valuable guidance resource as called for in part 1.0, Framework Introduction. Our organization already draws upon the existing standards, guidance, and best practices included in the Cybersecurity Framework in crafting our risk-based cybersecurity protection and mitigation efforts.

MidAmerican Energy Holdings Company is deeply engaged in the energy sector, with multiple operating companies in the natural gas and electric subsectors. Different lead sector agencies have provided varying and sometimes conflicting security guidance and programs. The proposed Framework includes provisions for each critical infrastructure sector to develop voluntary sector-specific implementation. Based o the language in sections C.3, Conformity Assessment and 1.2, Risk Management and the Cybersecurity Framework, we have identified potential concerns.

Our major concern is that voluntary Cybersecurity Framework best practices may be inappropriately applied beyond the original intent and scope. Our experience is establishing new protective cybersecurity technological or procedural controls may undermine existing protections if not executed in thoughtful, coordinated manner. The MidAmerican Energy Holdings Company cybersecurity programs have been specifically crafted based on risk assessment and available solutions to yield optimal results across disparate energy subsectors such as electric and natural gas. There is real risk in uncoordinated or rushed sector-specific implementation negatively impacting other sectors. The Cybersecurity Framework would be improved if a more refined, deliberative process for cross-sector coordination was elucidated in the document. Detailing the intra- and cross-sector coordination in Section 3.0, How to Use the Framework would underwrite future implementation, measurement and incremental improvement of the Cybersecurity Framework.

The concerns of poorly-coordinated implementation become even more acute if the Cybersecurity Framework is adopted as mandatory in certain sectors under regulatory law. Mandatory regulatory compliance removes the best practice and voluntary adoption elements clearly established in the Executive Order and drafts for the Cybersecurity Framework to date. Maintaining the strong voluntary character of the Cybersecurity Framework as described in Section 8 of the Executive Order is key to the

most flexible and rapid implementation. Use of the Cybersecurity Framework to voluntarily complement existing regulatory authorities is specifically only mentioned in line 677 of the present draft. We believe that the Cybersecurity Framework introduction should establish the voluntary aspect more clearly in the 1.0, Introduction and 2.3, Framework Implementation sections.