Donald F. Santa
President & CEO

October 15, 2012

The Honorable John D. Rockefeller IV
Chairman
Senate Committee on Commerce, Science and Transportation
254 Russell Senate Office Building
Washington DC 20510-6125

Dear Chairman Rockefeller:

The Interstate Natural Gas Association of America (INGAA) is a trade organization representing the vast majority of our nation's interstate natural gas transmission pipeline companies. We write today on behalf of our members in response to your September 19, 2012 letter to Fortune 500 companies that presented your concerns about the cybersecurity of our nation's privately owned infrastructure.

INGAA appreciates the attention you and your colleagues have brought to the protection of critical infrastructure from cyber-attack. As owners and operators of approximately 220,000 miles of interstate natural gas transmission pipelines, our infrastructure constitutes our business. Our members are especially motivated to utilize every safeguard and protection available to ensure our systems remain safe and reliable.

Since shortly after the September 11 attacks, INGAA and its members have worked with the federal government to develop, implement and update recommendations and best practices to improve the physical and cybersecurity of our nation's critical pipeline facilities. Because of these relationships, strong and productive standards, best industry practices and guidelines have been developed and implemented to benefit the nation's security.

For example, our members worked extensively with the Research and Special Programs Administration within the Department of Transportation (DOT) to develop the initial Pipeline Security Information Circular issued in September 2002. The circular established recommendations and best practices for improving security at critical pipeline facilities across the country. This collaborative approach to developing and implementing security measures continues to this day as part of our cooperative efforts with the Transportation Security Administration (TSA).

Interstate Natural Gas Association of America
20 F Street NW Suite 450
Washington, DC 20001
202-216-5900

After enactment of the Homeland Security Act of 2002 (P.L. 107-296) relocated TSA to the newly formed Department of Homeland Security (DHS), DHS assumed responsibility as the primary security regulator of interstate natural gas pipelines. As such, it has undertaken activities focused on national cybersecurity issues and engaged owners and operators of the nation's critical infrastructure on these issues. DHS's responsibilities are further reinforced by Homeland Security Presidential Directive 7 (HPSD-7, issued on Dec. 17, 2003), which requires DHS to "serve as a focal point for the security of cyberspace . . . ." Pursuant to HSPD-7, DHS, through the extensive coordination with its government security partners and the private sector, developed the National Infrastructure Protection Plan that outlines national goals, objectives, milestones and key initiatives necessary for fulfilling the Department's responsibilities for physical and cybercritical infrastructure protection across 18 critical infrastructure sectors. Under the authority of HSPD-7, DOT and DHS also established a Security Memorandum of Understanding and Annex between the Pipeline and Hazardous Materials Safety Administration and TSA.

Consistent with HSPD-7, TSA uses a voluntary partnership approach as it works with the private sector to leverage the collective expertise and experience of the government and private industry in finding practical solutions to cybersecurity. This approach, and the relationship it has fostered, has produced robust cybersecurity guidelines and best practices for natural gas transmission pipelines.

For example, this collaborative partnership resulted in the establishment of the Industrial Control Systems Joint Work Group (ICS-JWG). The ICS-JWG enhances the collaborative efforts of the industrial control systems stakeholder community in securing critical infrastructure by accelerating the design, development and deployment of secure industrial control systems. Cybersecurity is a particular focus for this group.

TSA's successful collaboration with the pipeline sector resulted in Pipeline Security Guidelines (April 2011), which include recommendations and best practices for both physical and cybersecurity of the nation's pipelines. These and other partnerships strengthen cyberprotection for our infrastructure because they are based on trust, peer-to-peer relationships and expertise in the operations of interstate transmission pipelines.

Much has been said about the need to empower federal agencies to develop cybersecurity standards for critical infrastructure such as pipelines. It is worth noting that the Aviation and Transportation Security Act of 2001 (P.L. 107-71) provides TSA with the authority to issue, rescind and revise such regulations as are necessary to carry out its functions. In addition, the 9/11 Act (P.L. 110-53) provides DHS the authority in section 1557 (d) to “develop and transmit to pipeline operators security recommendations” and if the Secretary “determines that regulations are appropriate….shall promulgate such regulations and carry out necessary inspection and enforcement actions.” Section 1557 (d) further provides that “[t]he regulations shall include the imposition of civil penalties for noncompliance.”

Thus, the federal agency responsible for the security of the nation's pipelines already has the authority to issue regulations – voluntary or mandatory – for cybersecurity matters. TSA's activities to date have been collaborative, with a focus on information sharing and voluntary industry compliance with security guidance and best practice recommendations.

This approach builds on what has been proven through experience – that a public-private partnership on cybersecurity is superior to mandated regulation. A Congressional Research Service August 2012 report, "Pipeline Cybersecurity: Federal Policy," stated that "TSA officials assert that security regulations could be counter-productive because they could establish a general standard below the level of security already in place at many pipeline companies based on their company-specific security assessments." Moreover, the report notes that "[b]ecause TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency believes it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well."

INGAA agrees with these comments. INGAA members have a strong record of working voluntarily and successfully with TSA to develop, maintain and update effective cybersecurity guidelines, which have been implemented across our industry. Most notably, our members diligently continue to assess vulnerabilities that can be addressed in future updates.

Unlike this dynamic approach, a regulatory regime that requires notice and comment rulemaking would be unable to keep pace with the ever-changing cyber threats and vulnerabilities emerging globally. The key to effective cybersecurity is the trust developed in a strong private sector partnership with law enforcement and intelligence agencies, as well as with the TSA. This is not possible when government cybersecurity regulators merely enforce federal regulation with civil penalties. The cybersecurity world moves too quickly for such a traditional regulatory model to be beneficial or productive.

Rather than focusing on new regulatory authority, INGAA supports federal action that could result in enhancing information-sharing opportunities and tools between national security agencies and the owners and operators of critical infrastructure. We believe that fostering these public-private partnerships is the most effective means for securing our nation's critical infrastructure and addressing any cyberthreats.

Respectfully,

Donald F. Santa