Dave McCurdy
President and CEO
American Gas Association

House Committee on Energy & Commerce Hearing
"Cyber Threats and Security Solutions" (May 21, 2013)

Response to Additional Question for the Hearing Record

The Honorable Anna G. Eshoo: If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?

The American Gas Association (AGA) believes that there is a role for cybersecurity legislation, particularly as it relates to improving public-private cybersecurity information sharing and related liability protections. Passing legislation that addresses both policy areas is of paramount concern.

To help counter cyberattacks and protect networks against future incursions, critical infrastructure, including natural gas utilities, needs government to help them identify, block and/or eliminate cyberthreats as rapidly and reliably as possible. From a functional perspective, this will require streamlining the process by which actionable threat intelligence is shared with private industry. Harnessing the cybersecurity capabilities of the government intelligence community on behalf of private sector networks will go a long way towards overall network security. The recently passed H.R. 624, *The Cyber Intelligence Sharing and Protection Act* (CISPA) provides a positive roadmap by establishing a cybersecurity partnership between critical infrastructure and the defense/intelligence community and DHS to distribute cyberthreat information, interpret and share potential threat impacts, and work with critical infrastructure to keep their networks safe. We hope that the Senate will move forward with the CISPA concept to improve our chances of getting a cybersecurity information sharing bill enacted into law.

Another avenue for legislation surrounds offering liability protection for companies with robust cybersecurity programs – standards, products, processes, etc. The Administration's recent executive order (EO) on cybersecurity underscores this need. The EO directs sector agencies, and the intelligence and law enforcement community to establish a cybersecurity information sharing partnership; tasks the National Institute of Standards and Technology with establishing a quasi-regulatory set of cybersecurity standards (a "cybersecurity framework"); and orders DHS to incentivize critical infrastructure to adhere to the NIST standards. What the EO cannot do is provide liability protections for critical infrastructure entities that make the effort to participate in a public-private cybersecurity program, regardless of whether it is created via EO or some future law.

AGA supports employing the *SAFETY Act* as an appropriate avenue for providing companies that participate in a government-private industry cybersecurity partnership with liability coverage from the impacts of cyberterrorism. *SAFETY Act* applicability in this area is plain:

- The SAFETY *Act* exists in current law, and a related office at DHS has been reviewing and approving applications for liability coverage in the event of an act of terrorism or cyber attack for over a decade. This office utilizes an existing review and approval process which would allow for immediate granting of liability protections from cyber attacks.
    - Because the *SAFETY Act* can apply to a variety of areas ranging from cybersecurity standards (cyber best practices, etc.), to procurement practices and related equipment (SCADA, software, firewalls, etc.) companies can layer their liability protection.
    - We are aware of no other existing statute that offers similar liability protections. Moreover, we do not see the need to write new law to address liability protections from cyber incidents when the *SAFETY Act* is already applicable.

This said, there are some areas where we believe the *SAFETY Act* could be a little stronger as it applies to cyber matters. First, and foremost, the statute could be expanded to make specific reference to liability protections from "cyber" events (cyber attacks, cyber terrorism, etc.) and more specific reference to coverage for cybersecurity equipment, policies, information sharing programs, and procedures. While there is coverage under the Act currently for cyber attacks, specifically identifying "cyber attacks" as a trigger for liability protections would strengthen the overall concept.

Congresswoman Eshoo, we hope that our response to your inquiry is sufficient and substantive. If you have any additional questions about our industry's cybersecurity priorities and activities, please contact Brian Caudill (bcaudill@aga.org), AGA's Senior Director of Federal Affairs at 202-824-7029.

400 N. Capitol St. NW 4th Floor, Washington, DC, 20001 **P:** 202-824-7029 **F:** 202-824-7092 **E:** bcaudill@aga.org **www.aga.org**