Hon. Dave McCurdy
President & CEO

Dave McCurdy
President and CEO
American Gas Association

Testimony before the House Committee on Energy & Commerce
"Cyber Threats and Security Solutions"

May 21, 2013

Chairman Upton, Ranking Member Waxman, and Members of the Committee, I am Dave McCurdy, President and CEO of the American Gas Association. Also relevant to this hearing, I am a former Chairman of the House Intelligence Committee and have been involved in cybersecurity policy for over 20 years. Thank you for inviting me to share my perspectives on critical infrastructure cybersecurity.

AGA represents more than 200 local energy companies that deliver natural gas to more than 71 million residential, commercial and industrial gas customers in the United States. AGA is an advocate for local natural gas utility companies and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international gas companies and industry associates. Today, natural gas meets almost one-fourth of U.S. energy needs.

Natural gas is the foundation fuel for a clean and secure energy future, providing benefits for the economy, our environment and our energy security. Alongside the economic and environmental opportunity natural gas offers our country comes great responsibility to protect its distribution pipeline systems from cyber attacks. Technological advances over the last 20 years have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected, more efficient industry is that we have become an attractive target for increasingly sophisticated cyber terrorists. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a

400 N. Capitol St. NW 4th Floor, Washington, DC 20001 P 202-824-7111 F 202-824-7098 E dmccurdy@aga.org www.aga.org

successful ongoing cybersecurity partnership with the Federal government.

Government-Private Partnerships & Cybersecurity Management: A Process that Works for Natural Gas Utilities

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. This said, industry operators recognize there are inherent cyber vulnerabilities with employing web-based applications for industrial control and business operating systems. Because of this, gas utilities adhere to myriad cybersecurity standards and participate in an array of government and industry cybersecurity initiatives. However, the most important cybersecurity mechanism is the existing cybersecurity partnership between the federal government and industry operators. This partnership fosters the exchange of vital cybersecurity information which helps stakeholders adapt quickly to dynamic cybersecurity risks.

Background: *The Homeland Security Act of 2002* provides the basis for Department of Homeland Security (DHS) responsibilities in protecting the Nation's critical infrastructure and key resources (CIKR). The Act assigns DHS the responsibility for developing a comprehensive plan for securing CIKR. This plan, known as the National Infrastructure Protection Plan (NIPP), identifies 18 critical infrastructure sectors within which natural gas transportation is a subsector of the Energy and Transportation Sectors. The NIPP states that more than 80 percent of the country's energy infrastructure is owned by the private sector, and that the Federal Government has a statutory responsibility to safeguard critical infrastructure. For this reason, information-sharing amongst industry operators and the government intelligence community is critical to cyber infrastructure protection.

AGA-Government Cybersecurity Partnerships: Natural gas utilities work with government at every level to detect and mitigate cyber attacks. In particular, AGA works closely with the Transportation Security Administration, Pipeline Security Division, the government entity designated to oversee physical and cybersecurity operations of distribution pipelines. AGA views our relationship with TSA as a true partnership that benefits all stakeholders because it allows government and pipeline owner/operators to exchange

cybersecurity information typically not shared in a regulatory compliance-driven environment. In addition, gas utilities collaborate with the DHS *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) on cybersecurity awareness, detection, and mitigation programs. This process calls on operators to submit suspicious cyberactivity reports to ICS-CERT. In turn, ICS-CERT advises operators of cyber vulnerabilities, mitigation strategies, and forensic analyses. This open communication bolsters the industry's overall cybersecurity posture, and advances ICS-CERT's mission. Simply put, ICS-CERT understands cyber threats; natural gas utilities understand their operations; and the two work in tandem to protect targeted critical infrastructure.

AGA also strongly encourages industry participation in DHS-led training programs and system evaluation programs, as well as relevant cybersecurity programs operated by other agencies. Moreover, DHS officials regularly meet with industry groups, such as the AGA Board of Directors and individual member companies, to review and assess ongoing cyberthreats. Bottom line, as cybersecurity threats to gas industry operations have evolved, there has been a corresponding improvement in how gas utilities respond to these threats due to our substantive cybersecurity partnership with DHS.

The following is a list of additional government-natural gas industry cybersecurity partnerships:

- *DHS Cybersecurity Briefings.* Industry operators participate in DHS briefings to receive threat and risk information and analytics. The briefings provide information on the state of the ONG sector in reference to emerging threats, security incidences, and trends. AGA is leading the collaborative effort between the government intelligence community and private industry to improve on timely, credible, and actionable information sharing.

- *DHS Control Systems Security Program*. DHS offers industry operators opportunities to enhance their knowledge of control system cybersecurity via ICS-CERT training, online forums, recommended practices, advisories, and interactive live assistance. Industry operators also receive *United States*

Computer Emergency Readiness Team (US-CERT) activity summaries and advisory communications; submit incident reports for analysis; and engage in the Industrial Control Systems Joint Working Group for information exchange.

- *Oil & Natural Gas Sector Coordinating Council (ONG SCC) Cybersecurity Working Group.* Industry operators participate in this DHS-sponsored forum for coordination of ONG cybersecurity strategy, policy, and communication. The ONG SCC provides a venue for operators to mutually plan and execute sector-wide cybersecurity programs, exchange information, and assess progress toward protecting ONG sector critical infrastructure.

- *TSA Cyber Security CARMA Program.* Sponsored by TSA, this program seeks to develop a national cyber risk management framework to help industry identify where internal risk management activities align with industry-wide risk management activities. AGA co-chairs this collaborative effort and facilitates operator participation and contribution.

- *Coordinate Federal Government Risk Assessment Programs.* AGA coordinates meetings with the Department of Energy, Federal Regulatory Energy Commission, TSA, and ICS-CERT to encourage government entities to align various cybersecurity risk assessment programs. The objective is to compare/contrast the programs and identify useful synergies.

AGA-Industry-Government Cybersecurity Guidelines: Partnership between the private sector and the government is critical to address cybersecurity threats to critical infrastructure. As such, AGA and industry operators also collaborate with government partners to produce effective cybersecurity practices and guidelines. Below are a few examples.

- *Transportation Security Administration, Pipeline Security Guidelines.* Guidelines developed through a collaborative effort of government and pipeline asset owners. Used by natural gas pipeline companies,

natural gas distribution companies, and liquefied natural gas facilities as a framework to protect critical/non-critical pipeline infrastructure. AGA served as a subject matter expert in drafting the cybersecurity chapter.

- *DHS Control Systems Security Program, Cyber Security Evaluation Tool (CSET).* A software tool that guides users through a step-by-step process to assess the cybersecurity posture of industrial control systems and information technology networks. AGA participated in the development, testing, and distribution of this material and contributes regular updates.

- *Department of Energy, Roadmap to Achieve Energy Delivery Systems Cybersecurity*. A framework to improve cybersecurity within the energy sector via a collaborative vision of industry, vendors, academia, and government stakeholders. The framework includes goals and deadlines over the next decade. AGA has contributed to this resource since 2006.
- *Interstate Natural Gas Association of America (INGAA), Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry.* Guidelines designed to assist natural gas pipelines in managing control system cybersecurity requirements. Aligns with TSA Pipeline Security Guidelines and other standards used across the oil and natural gas industries. AGA reviewed its development and promotes it as a valuable resource to member companies.
- *AGA and INGAA, Security Practices Guidelines, Natural Gas Industry Transmission and Distribution*. Guidelines that provide recommended cybersecurity practices and procedures for transmission and distribution segments of the natural gas industry. AGA and INGAA developed this guidance for natural gas pipeline and utility operators.

Non-Standardization of Cybersecurity Practices is Paramount

In the recent past, concerns over increasing cyberattacks on critical infrastructure have led to legislative efforts

to create a set of top-down cybersecurity regulations. AGA remains concerned that prescriptive cybersecurity regulations will have little practical impact on cybersecurity and, in fact, will hinder implementation of robust cybersecurity programs. First and foremost, prescriptive cybersecurity regulations would fundamentally transform the productive cybersecurity relationship natural gas utilities have with the TSA Pipeline Security Division from a successful partnership to a more standard regulator-regulated mode, forcing companies to focus more resources on compliance activities than on cybersecurity itself. Also, from a practical perspective, it is unlikely that any set of cybersecurity regulations will be dynamic enough to help companies fight constantly changing and increasingly sophisticated threats.

Across the natural gas industry, cybersecurity effectiveness is maximized through the diversity of individual company cybersecurity approaches, e.g. Defense in Depth strategies and customized detection and mitigation systems appropriate for individual company networks. Companies also turn lessons learned from government-private industry cybersecurity information sharing partnerships into actions designed to protect their specific systems. In sum, as cybersecurity risks and threats change, so do vulnerabilities. Ongoing implementation of new and diverse cybersecurity tools and procedures, based on unique individual company requirements, helps companies adapt to a dynamic cyberthreat environment and bolsters overall gas utility industry cybersecurity.

The Cybersecurity Executive Order, Private Sector Perspective

The Administration's Executive Order (EO), *Improving Critical Infrastructure Cybersecurity* establishes national policy on critical cyber infrastructure security. Because the EO's direct impact on private sector cybersecurity programs is significant, AGA, AGA's multi-company Cybersecurity Strategy Task Force and individual companies have been working collaboratively with government stakeholders on the various EO directives since its release. In addition, AGA chairs a joint cybersecurity working group of the Oil & Natural Gas, Pipeline and Chemical Sector Coordinating Councils, a working group established specifically to address EO activities. As such, AGA is uniquely situated to share insight received from multiple sectors.

In general, we believe the EO's voluntary process is the right approach and we actively participate in the working groups that lead DHS' coordination of interagency and public and private sector efforts in implementing the EO. These working groups include, Stakeholder Engagement, Cyber-Dependent Infrastructure Identification, Planning and Evaluation, Situational Awareness and Information Exchange, Incentives, Cybersecurity Framework Collaboration (with NIST), Assessments of Privacy and Civil Rights and Civil Liberties, and Research and Development. The working groups have sponsored constructive work sessions with stakeholders, including gas utilities. Moreover, DHS has made a substantive effort to address industry concerns about true public-private collaboration, technical expertise, transparency, and scheduling.

Overall, the EO is simply the beginning of a long march to improve national cybersecurity. AGA is hopeful, and will work to ensure that throughout this process gas utility cybersecurity concerns will be addressed. Below are a few of our specific concerns and observations.

Identifying Critical Infrastructure. The executive order confines itself largely to "critical infrastructure", defined in Section 2 of the EO as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."* From the start, AGA has suggested that the identification process include the informed participation of critical infrastructure owner/operators. And while the government has acceded to this industry wish, the results to date have been mixed.

A general stakeholder concern at every working session is that the EO process is hurried and that the tight timelines require DHS to value rapidity more than process and content, making it difficult for proper assessment and vetting of information. Notably, the Cyber-Dependent Infrastructure Identification (CDII) process has suffered in this process. While it appears that DHS is acting prudently, identifying only cyber infrastructure at 'greatest risk' of resulting in catastrophic consequences if compromised, the criteria proposed for that

identification process continues to morph without transparency and consultation with stakeholders.

Since 2007, DHS has used criteria listed in the National Critical Infrastructure Prioritization Program (NCIPP) to identify and prioritize critical infrastructure that could through destruction or disruption have catastrophic national or regional consequences. The identified assets provide the foundation for infrastructure protection and risk reduction programs executed by DHS and its public and private sector partners. Unfortunately, as part of the EO's new CDII process, when natural gas owner/operators assessed their operations using the NCIPP criteria and arrived to conclusions that their infrastructure was not at 'greatest risk', DHS changed the criteria without notice, comment or collaboration. Natural gas owner/operators also participated in the DHS-developed Cybersecurity Assessment & Risk Management Approach Model (CARMA), a risk evaluation process that assesses cybersecurity risks that stakeholders and task force leaders agreed would be relevant to the EO's CDII process. Again, after evaluation, conclusions show that sector infrastructure is not at the 'greatest risk'. Furthermore, this analysis matches internal assessments performed by various industry trade associations.

Clearly there is disagreement within sector specific agencies (DHS, DOE, etc.) about whether or not natural gas facilities should be considered critical cyber-dependent infrastructure. For natural gas entities, which answer to multiple sectors specific agencies, this is unsettling. Regardless the ultimate answer, we remain hopeful that the government-industry CDII partnership will decide this question in an open, collaborative and scientific fashion.

Cybersecurity Information Sharing Program. Section 4 of the EO creates a cybersecurity information sharing program, directing DHS, the Department of Justice, and the Office of the Director of National Intelligence to set up cyber threat information sharing processes with targeted private sector entities. Without question, improved information sharing can and will benefit critical infrastructure cybersecurity. However, for industry to fully engage in an information sharing program, information protection mechanisms (safe harbors) and liability protections must be afforded to owners/operators who participate in the program. Without such protections, companies may be unwilling to participate because of the possibility of information leaks as well as due to

competitive concerns and legal liability pressures.

NIST "Cybersecurity Framework". Section 7 of the EO directs the National Institutes of Standards and Technology (NIST) to develop, via an open review process, a "Cybersecurity Framework" designed to improve critical infrastructure cybersecurity. The Framework will utilize risk and performance based standards/best practices; technology neutral applications; voluntary consensus standards and industry best practices; and cross-sector security standards applicable to all critical infrastructure. Ultimately, NIST's goal is to create a framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective" to help critical infrastructure owner/operators manage cyber risk.

At present, NIST's Cybersecurity Framework development process appears headed in the proper direction, primarily due to internal technical expertise and substantive stakeholder involvement. However, an upcoming stakeholder workshop (May 29-30) will be the determining factor as to what extent industry comments are incorporated into the final product. Our primary concerns with the voluntary Framework are:

- The Framework development process largely ignores time-tested and effective information sharing partnership efforts between the public and private sectors over the past several years – most notably the gas industry's existing cybersecurity partnership with TSA, ICS-CERT, etc.

- Framework provisions must remain flexible and not morph into mandated regulations, which will quickly become outdated due to an ever-changing cyber threat landscape.

- Framework inflexibility will also create vulnerabilities in intricate systems tailored to specific company operations and risk profiles. That is, simply building more defenses is no longer effective; the focus has shifted to increased monitoring and better and faster incident response, which requires robust cybersecurity programs and effective information sharing.

Overall, AGA appreciates the opportunity to participate in a standards development process that has potential to impact our cybersecurity programs. We look forward evaluating the final product on its merits. Ultimately, if there is a valid basis for its incorporation and/or the Framework does not conflict with existing domestic and international cybersecurity standards and/or regulations, gas utilities will be strongly encouraged to adopt it.

Industry Adoption of Cybersecurity Framework. Section 8 of the EO directs DHS to create a "voluntary" program to spur critical infrastructure entities to adopt the NIST Framework Specifically, DHS will work with other agencies to review the Framework and develop implementation guidance to address sector-specific operating environments. More importantly, DHS will work with the Departments of Commerce and Treasury to report on existing incentives that might spur industry participation in the voluntary program as well as any additional incentives (i.e. liability protections) that would require new statutory authority. Sector agencies will also report annually on which critical infrastructure owner/operators participate in the program. Overall, just how "voluntary" this program ends up becoming is an open question. As AGA and other critical infrastructure industries have argued, voluntary government programs often morph into de facto mandatory compliance programs because companies feel compelled to participate rather than risk opening themselves up to litigation for not engaging in a program that has the imprimatur of the federal government.

This program for incentivizing participation in the NIST Framework does create concerns. First of all, many of the proposed incentives are basic activities the government should already be providing under any reasonable public/private cybersecurity partnership. More importantly, if some entities ultimately decide to not adopt the voluntary NIST Framework, it is neither appropriate nor necessary to incentivize their participation (or punish non participation) by offering/not offering "incentives" such as favored status in government contracting, greater access to cybersecurity training and support, expedited security clearances and the like. Fact is, without new statutory authority to provide meaningful incentives like information-sharing safe harbors for entities that share cybersecurity information with the government and liability protections for companies with robust cybersecurity programs, there is a limit to what the government can do to entice companies to participate in

the Framework.

More significant, measurable, and non-controversial than incentives would be increasing opportunities for companies to request government cyber readiness appraisals and assistance in the event of a system compromise. This can be done by reinforcing support for existing highly-regarded programs such as DHS ICS-CERT red team/blue team training and onsite cybersecurity evaluations, and the Department of Energy's Cybersecurity Capability Maturity Model onsite testing. The vast majority of natural gas utilities are already taking serious steps, commensurate with the known risks, to protect their systems from cyberthreats. These companies have a continuing interest in knowledge relating to new threat vectors, indicators and mitigation measures, and don't need incentives or direct federal involvement to help manage their cyber vulnerabilities.

Agency Adoption of NIST Cybersecurity Framework. Section 10 of the EO notes that once the NIST Framework has been preliminarily drafted agencies with cybersecurity regulatory responsibilities will review their existing authorities to determine whether they are sufficient given the cyberthreat landscape, and whether they can implement the NIST Framework via regulation. If agencies determine that their current cybersecurity regulatory requirements are insufficient then they shall propose new "actions" to mitigate cyber risks. This section clearly pushes sector agencies to create new cybersecurity regulations. These new requirements would, at a minimum, be based upon the NIST Cybersecurity Framework; however, there is plenty of suggestion in Section 10 that agencies move beyond the framework, or seek the authority to do so. We are hopeful this will not lead to regulation for regulations sake. For example, despite having the statutory authority necessary, TSA Pipeline Security Division has chosen not to issue cybersecurity regulations for natural gas utilities in large part because of the successful security partnership we have collectively developed.

The Case for Cybersecurity Legislation.

Despite our concerns about prescriptive cybersecurity standards, AGA does believe that there is a role for

cybersecurity legislation, particularly as it relates to improving public-private cybersecurity information sharing and related liability protections.

Information Sharing. To help counter cyberattacks and protect networks against future incursions, critical infrastructure 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.

Liability Protection, *SAFETY Act*. 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, 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 seems 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.

THE NATURAL GAS UTILITY CYBERSECURITY POSTURE

AGA's policy priorities for cybersecurity include preserving our current cybersecurity partnership with the Transportation Security Administration, Pipeline Security Division, enhancing government-private industry cybersecurity information sharing, opposing burdensome or counterproductive cybersecurity regulation, and supporting robust liability protections for entities that are serious about protecting their networks. If ultimately achieved, these items will only bolster an already solid industry cybersecurity commitment.

America's natural gas utilities are cognizant of enduring cyber threats and the continued need for vigilance through cybersecurity protection, detection, and mitigation mechanisms. There is no single solution for absolute system protection. However, through a combination of cybersecurity processes and timely and credible information-sharing amongst the government intelligence community and industry operators, America's natural gas delivery system remains protected, safe and reliable, and will remain so well into the future.