

DANIEL K. INOUE, HAWAII
JOHN F. KERRY, MASSACHUSETTS
BARBARA BOXER, CALIFORNIA
BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
FRANK R. LAUTENBERG, NEW JERSEY
MARK PRYOR, ARKANSAS
CLAIRE McCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
TOM UDALL, NEW MEXICO
MARK WARNER, VIRGINIA
MARK BEGICH, ALASKA

KAY BAILEY HUTCHISON, TEXAS
OLYMPIA J. SNOWE, MAINE
JIM DEMINT, SOUTH CAROLINA
JOHN THUNE, SOUTH DAKOTA
ROGER F. WICKER, MISSISSIPPI
JOHNNY ISAKSON, GEORGIA
ROY BLUNT, MISSOURI
JOHN BOOZMAN, ARKANSAS
PATRICK J. TOOMEY, PENNSYLVANIA
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE
DEAN HELLER, NEVADA

ELLEN DONESKI, STAFF DIRECTOR
BRIAN M. HENDRICKS, REPUBLICAN STAFF DIRECTOR AND GENERAL COUNSEL

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEB SITE: <http://commerce.senate.gov>

May 24, 2012

Mr. Dave McCurdy
President and Chief Executive Officer
American Gas Association
400 N. Capitol St., NW #450
Washington, DC 20001

Dear Mr. McCurdy,

Since early 2009, in my capacity as Chairman of the Senate Committee on Commerce, Science, and Transportation, I have been working to address our nation's cyber vulnerabilities, particularly those vulnerabilities in our most critical infrastructure. As a former Chairman of the Senate Intelligence Committee, I am well aware of both the gravity and likelihood of cyber threats that could do great damage to the United States. The recent cyber attacks that targeted your industry remind all of us that these threats are real and that we must take steps to protect our country from threats to critical infrastructure.

The companies that make up your association play a critical role in our country's economy and the daily lives of millions of Americans. Natural gas meets almost one-fourth of our country's energy needs and there are more than 70 million residential, commercial, and industrial natural gas customers nationwide.¹ Many Americans likely take for granted the service your industry provides, given its dependability and ubiquity. A prolonged disruption to this energy supply, whether through a cyber attack or other catastrophe, would be disastrous.

The American Gas Association (AGA) has recognized these dangers as well, as it has worked to understand the cyber vulnerabilities within the control systems that utilities and pipelines are dependent upon. Your organization published a report as early as March 2006 that noted "there are credible [cyber] vulnerabilities that threat agents could exploit."² The report found:

With little effort, an attacker can scan the communication links between remote sites, as well as between remote sites and control centers. Access also can be gained through back channels used to establish field device operational settings

¹ American Gas Association, *American Gas Association Overview* (online at <http://www.aga.org/Newsroom/factsheets/Documents/AGA%20Overview%20Fact%20Sheet%20%28JAN%202012%29.pdf>) (accessed May 22, 2012).

² American Gas Association, *Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan* (Mar. 14, 2006) (AGA 12, Part 1) (online at <http://www.aga.org/our-issues/security/Documents/0603REPORT12.pdf>).

and to modify field device software. In a control center, many SCADA systems write data to a master station database, which then is read by others to perform a wide variety of business functions. This interface also may be compromised, giving the attacker access to either SCADA operations or to sensitive data used by business operations.³

Based upon these findings, an AGA working group developed a set of standards, known as “AGA-12,” to protect the data transmitted by control systems. These measures were eventually tested and supported by both government agencies and private organizations, including the Department of Energy and the Gas Technology Institute.⁴

While your industry should be commended for working to recognize its cyber vulnerabilities, I am concerned about a recent press report which suggested that “AGA-12” was abandoned because of the costs.⁵ One independent researcher who helped develop “AGA-12” stated the following:

What I think killed AGA-12 more than anything else was the cost of it. It was a success. But nobody was willing to pay \$500 for a bump in the wire solution even if it radically improved security. I haven’t seen any deployment of it.⁶

Other industries with critical infrastructure have faced the same choice as well. While many companies wisely view enhancing cybersecurity as a good long-term investment for owners and operators of critical infrastructure, some companies have chosen to view it as a short-term expense and have not taken the necessary steps to protect their critical business assets. Other companies are simply unaware of cyber risks and the steps they should take to protect their systems.

It has been widely known for years that our critical infrastructure is vulnerable and that the threats are real. Yet, while the threats have grown, the vulnerabilities remain. I fear that the business justification for securing critical infrastructure will not come until it is too late, after a cyber attack does great damage to our economy, or worse, causes a mass casualty event. At that point, the private sector will have little choice but to make the necessary investments in cybersecurity.

³ *Id.*

⁴ Mark Hadley, Kristy Huston, *AGA 12, Part 2 Performance Test Plan*, U.S. Department of Energy Office of Electricity Delivery and Energy Reliability (Nov. 2006) (online at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/AGA_12_Part_2_Performance_Test_Plan.pdf); William F. Rush, John A. Kinast, and Aakash B. Shah, *AGA 12 Recommends How To Protect SCADA Communications From Cyber Attack*, Pipeline & Gas Journal (Nov. 2006) (online at <http://igs.nigc.ir/igs/OTHER/AGA-12-SCADA.PDF>).

⁵ Mark Clayton, *Cybersecurity: How US utilities passed up chance to protect their networks*, The Christian Science Monitor (May 17, 2012) (online at <http://www.csmonitor.com/USA/2012/0517/Cybersecurity-How-US-utilities-passed-up-chance-to-protect-their-networks>).

⁶ *Id.*

Letter to Mr. McCurdy
May 24, 2012

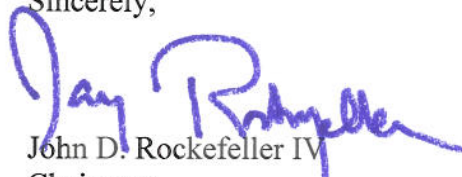
For these reasons, I have advocated for cybersecurity legislation that creates a partnership between the private sector and the federal government to address our nation's critical infrastructure cyber vulnerabilities. The private sector and the federal government would work together to create minimum cybersecurity protections for critical infrastructure that companies would achieve using the methods they themselves deem most appropriate. Until this legislation becomes law, it remains solely a company's private choice to protect critical infrastructure and companies have frequently chosen not to take the proper steps.

To help me better understand the decisions your industry has made with respect to cybersecurity, I ask that you provide responses to the following questions:

1. Why did the American Gas Association create the AGA-12 Cryptography Working Group?
2. What standards did the AGA-12 Cryptography Working Group create?
3. Were these standards implemented? If not, why not?
4. In a report (AGA Report No. 12, Part 1), the working group referenced cyber vulnerabilities in control systems that utilities are dependent upon. Have the vulnerabilities been addressed?
5. Since 2006, has the American Gas Association created any additional standards or guidelines related to cybersecurity? If so, what are those standards or guidelines?
6. Does the American Gas Association have any mechanism which ensures its member companies follow the cybersecurity standards or guidelines it creates?

Please provide responses by Thursday, June 7, 2012. If you have any questions, contact Erik Jones with the Committee staff at (202) 224-1300.

Sincerely,



John D. Rockefeller IV
Chairman