AGA
American Gas
Association

April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The American Gas Association (AGA) is pleased to submit comments in response to the Request for Information issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), in the Federal Register (78 FR 13024, pages 13024 - 13028) on February 26, 2013, seeking input on *Developing a Framework To Improve Critical Infrastructure Cybersecurity*.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 71 million residential, commercial and industrial natural gas customers in the U.S., of which 92 percent — more than 65 million customers — receive their gas from AGA members. 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 the United States' energy needs. For more information, please visit www.aga.org.

AGA surveyed a number of its natural gas distribution and transmission utility companies, and their collective comments are incorporated below.

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and their management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/ or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

A survey of AGA members identified the following as what is currently seen to be the greatest challenges in further improving cybersecurity practices:

- Availability of specific, actionable and timely threat and attack information from government sources
- Availability of vulnerability information and indicators of compromise so mitigation measures can be implemented
- Lack of a common set of security practices that vendors and consultants adhere to when providing critical infrastructure products and services
- Lack of commerce controls for supply chain when procuring products and services from foreign countries
- Ability to use federal government agencies for background investigations of employees operating in sensitive roles
- Availability of a risk management and compliance framework that is based on risk outcomes versus compliance mandates and objectives
- Developing a framework that provides meaningful risk reduction without creating overly burdensome or unnecessary reporting and compliance efforts
- Development of a comprehensive framework applicable across a diverse set of critical infrastructures and assets
- Cybersecurity practices that become regulations and shift the focus from protection to compliance and demonstration of proof of compliance
- Lack of cybersecurity technology for proprietary assets
- Lack of available personnel with skill sets that include knowledge of utility operations and cybersecurity
- Ensuring that employees are trained and aware of the criticality of their role and responsibility in cybersecurity
- The variety of distinct cybersecurity requirements that federal or state regulatory bodies may require

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

The leading challenge observed by AGA member survey respondents is government's lack of recognition of the uniqueness of the various critical infrastructure sectors. Security measures deemed essential to one may not be essential to others, and the development of a framework applicable to a diverse set of assets must recognize that there should not be a universal level of protection for all assets.  Further, prescriptive security controls at a low detailed level will result in standards that become outdated as threats and technologies rapidly evolve which may yield a less secure infrastructure. Coordinating across sectors will be a challenge, but we must be vigilant to put a framework in place that improves cybersecurity rather than just catering to the least common denominators.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

Cybersecurity risk has been identified as one of the highest priorities for AGA member companies. AGA member survey respondents rely on enterprise risk management (the methods and processes used by organizations to manage risks). Some employ the Committee of Sponsoring Organizations Internal Control – Integrated Framework.  In most AGA member company survey respondents, cybersecurity risk is ultimately overseen by their respective senior executive leadership and Board of Directors. The enterprise risk management function is responsible for communicating corporate risk messaging across the organization. In addition to risk management, incident response is also a crucial element of cybersecurity incident management, which is integrated into company emergency operations plans.

In support of the natural gas distribution industry, AGA has several communications networks.  The Natural Gas Security Committee, Cybersecurity Strategy Task Force, Cybersecurity Mailing List, and AGA website (www.aga.org) provide avenues for communication and information dissemination.  When risk, threat and mitigation information is made available to AGA, it is shared broadly with our members.

4. Where do organizations locate their cybersecurity risk management program/office?

AGA member survey respondents locate cybersecurity risk in one of several corporate areas: the General Counsel's office, the Information Technology organization, and/or an Enterprise Risk Management group. Ultimately the cybersecurity function reports to senior executive management which reports to the chief executive officer and the Board of Directors.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

AGA member survey respondents evaluate risk based on loss and/or negative outcomes of financial and non-financial events. A risk is assessed based on measurement of the effectiveness of controls in place to manage that risk.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

AGA member survey respondents incorporate cybersecurity risk management into enterprise risk management and identify cybersecurity risk as one of the highest risks to the organization.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

AGA member survey respondents have adopted best practices such as defense in depth and use cybersecurity standards from industry, academia and government sources, such as TSA, DHS, NIST, SANS, AGA, and INGAA.

Below are specific titles related to cybersecurity. There are regulations, standards, guidelines, best practices and tools pertaining to the operations of natural gas utility companies that are not included in this list.

Interstate Natural Gas Association of America (INGAA), Control Systems Cyber Security Working Group, Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry, January 31, 2011

American Gas Association (AGA) Report 12, Cryptographic Protection of SCADA Communications: Part 1: Background, Policies and Test Plan (AGA 12, Part 1), March 14, 2006

AGA and Interstate Natural Gas Association of America (INGAA), Security Practices Guidelines Natural Gas Industry Transmission and Distribution, May 2008

American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-2010, (IEC 62264-1 Mod) Enterprise-Control System Integration Part 1: Models and Terminology, approved May 13, 2010

ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Part I: Terminology, Concepts, and Models, Oct. 2007

ANSI/ISA-99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, Jan. 13, 2009

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2005, Information Technology — Security Techniques — Information Security Management Systems — Requirements

ISO/IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management

Department of Homeland Security (DHS) Control Systems Security Program, Cyber Security Evaluation Tool (CSET)

DHS, National Cyber Security Division, Control Systems Security Program, Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011

DHS, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009

DHS, Cyber Security Procurement Language for Control Systems, Sept. 2009

DHS Transportation Security Administration (TSA), Pipeline Security Guidelines, Dec. 2010

DOE/The President's Critical Infrastructure Protection Board, 21 Steps to Improve Cyber Security of SCADA Networks

National Institute of Standards and Technology (NIST), SP 800-16 Revision 1, Draft Information Security Training Requirements: A Role- and Performance-Based Model, Mar. 20, 2009

NIST, SP 800-36: Guide to Selecting Information Technology Security Products, Oct. 2003

NIST, SP 800-48 Rev 1: Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008

NIST, SP 800-50: Building an Information Technology Security Awareness and Training Program, Oct. 2003

NIST, SP 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005

NIST, SP 800-53 Revision 3: Recommended Security Controls for Federal Information Systems and Organizations, August 2009

NIST, SP 800-53A Revision 1: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, July 2010

NIST, SP 800-61 Revision 1: Computer Security Incident Handling Guide, Mar. 2008

NIST, SP 800-63, Version 1.0.2: Electronic Authentication Guideline, April 2006

NIST, SP 800-73-3: Interfaces for Personal Identity Verification, February 2010

NIST, SP 800-76-1: Biometric Data Specification for Personal Identity Verification, Jan. 2007

NIST, SP 800-82: Guide to Industrial Control Systems (ICS) Security, June 2011

NIST, SP 800-83: Guide to Malware Incident Prevention and Handling, Nov. 2005

NIST, SP 800-86: Guide to Integrating Forensic Techniques into Incident Response, Aug. 2006

NIST, SP800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Feb. 2007

The White House, The National Strategy to Secure Cyberspace, Feb. 2003

Consortium of Cybersecurity Action, Twenty Critical Security Controls, 2012

SANS Top 20 Critical Cybersecurity Controls, 2012

Other sources include ICS-CERT alerts and classified briefings from government agencies.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

We know of no direct federal cybersecurity regulatory reporting requirements for natural gas utility operations. TSA has primary authority over pipeline physical security and cybersecurity. It has instituted voluntary cybersecurity standards and works cooperatively with industry on cyber threats. Many AGA member survey respondents voluntarily report cybersecurity threat and attack information to ICS-CERT. Certain states have cybersecurity regulatory reporting requirements for state regulated natural gas utilities.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Natural gas utilities depend on transmission pipelines to deliver this fuel. This transportation process requires electricity and water for operating various components of compressor stations. Further, power generation for downstream electricity can depend on natural gas. All these functions depend on telecommunications for monitoring, information technology for remote operation and financial services for billing.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Many AGA member survey respondents have corporate goals which start at the organizational level with defining a corporate strategy that leads to goals and objectives. Performance goals (including safety and reliability) are developed at a strategic level and propagated down to the operational and individual contributor level. For some AGA member survey respondents, additional performance-based goals are provided by public utility commissions. Performance goals could be based on preparations/exercises (before the event) versus restoration (after the event). Performance-based risk management goals are often tied to reliability of service, safety, and cost to the end consumer.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

AGA member survey respondents report criminal cybersecurity incidents to state and/or federal authorities as may be required. When required, threats and vulnerabilities that may potentially lead to exposure of critical infrastructure systems and infrastructure are reported to state or federal law enforcement authorities. The data reported can be detailed vulnerability, threat and/or exploit information. Additionally, appropriate records of a potential or successful intrusion or incident can also be reported. Natural gas utilities diversified in electric, nuclear and/or dam operations must report to NERC, NRC and state dam offices. Coastal-based utilities report to USCG. Utilities that have chemical storage, such as liquefied natural gas, report to the Infrastructure Security Compliance Division. And pipelines report to DHS and TSA. Owner/operators of natural gas distribution companies tend to report cyber incidences to the DHS ICS-CERT, which does not serve a regulatory function and has developed a trusted relationship with the owner/operator to achieve a single common objective – incident mitigation.

12. What role(s) do or should national/international standards and organizations that develop national/ international standards play in critical infrastructure cybersecurity conformity assessment?

National and international standards and organizations that develop standards can play an important role by helping align and consolidate the multitude of existing and developing cybersecurity standards and regulatory requirements. Foreign and international laws should stipulate ownership and authority over enforcement actions, legal action, recourse, etc. Many of the attempted or successful breaches on US based systems originate from foreign countries where no current legal recourse exists, leaving organizations vulnerable to long-term exposure. Additionally, those standards should establish appropriate reporting requirements and procedures for information sharing as well as incident handling.

Use of Frameworks, Standards, Guidelines, and Best Practices As set forth in the Executive Order.

The Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.
NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

Please provide information related to the following:

1. What additional approaches already exist?

AGA has encouraged its members to utilize the TSA Pipeline Security Guidelines as appropriate, ICS-CERT guidance material, and cybersecurity guidelines developed by trade associations.

2. Which of these approaches apply across sectors?

ICS-CERT alerts and best practices and NIST standards apply across sectors.

3. Which organizations use these approaches?

AGA member survey respondents use a combination of the TSA Pipeline Security Guidelines, the INGAA Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry, ICS-CERT alerts and best practices, other industry-developed guidelines, and NIST standards.

4. What, if any, are the limitations of using such approaches?

Some of these approaches focus on compliance objectives as opposed to risk outcomes. In addition, not all approaches are cost effective to all sectors or appropriate for all operators given the uniqueness of each company’s operating system.

5. What, if any, modifications could make these approaches more useful?

Stronger documentation of the available approaches would be helpful and would provide more flexibility for an organization to determine the most effective treatment of risk through a variety of possible controls. Owner/operators should be granted the flexibility to make the most prudent use of controls based on a high-level framework.

6. How do these approaches take into account sector-specific needs?

An appropriate Risk Management framework considers that risk areas are multi-dimensional and provides an appropriate construct for organizations to make risk mitigation decisions by applying the appropriate process and technology controls. This model provides the flexibility and scalability to be adaptable to any risk situation.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Standards development for use of existing frameworks should take into account sector specific issues and the diversity that can exist within a sector and remain voluntary to ensure asset owners are able to adapt existing robust cybersecurity programs to ensure reliable, safe and cost effective services.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The sector-specific agencies and related sector coordinating councils encourage companies to implement these approaches and best practices by fostering an information exchange and sharing environment. In addition, industry associations such as AGA promote collaboration among natural gas and other energy sector entities.

9. What other outreach efforts would be helpful?

Education, training and awareness in the form of workshops, webinars and tutorials are outreach efforts that would be helpful.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;

- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

These practices are mature and incorporated in documents such as TSA's Pipeline Security Guidelines and INGAA's Cybersecurity guidelines which are used by many AGA member survey respondents. The core practices identified by NIST are not unique to critical infrastructure. Enterprise Risk Management includes the following processes at a minimum that are common across many industries: Strategic Planning, Capital Planning, Project Planning, Development, Integration, Monitoring and Incident Response.

2. How do these practices relate to existing international standards and practices?

The core practices relate to existing international standards and practices in that they are applicable broadly to all industries.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Practices that AGA member survey respondents identified as especially critical would be: Separation of business from operational systems; Identification and authorization of users accessing systems; Monitoring and incident detection tools and capabilities; and Incident handling policies and procedures. All of these practices should be applied using a risk-based approach.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

At a high-level, the guidance and practices may be applied cross-sector. Organizations that operate critical assets should evaluate these practices using a risk-based approach to determine if the practice is applicable or not. Applicability of these practices may vary across organizations in a specific sector based on risk factors.

5. Which of these practices pose the most significant implementation challenge?

The challenges to implement these practices will vary across an organization in a given sector based on the current technology deployed, resource constraints and the regulatory requirements of a given organization. Specific to natural gas utilities, commonly used equipment in some natural gas industrial control system environments often do not support centralized authentication and access controls that are consistent with current technology standards.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Standards and guidelines are used to define how a given practice is applied to varying technology throughout an organization. Standards and guidelines also define the appropriate implementation and testing procedures to ensure controls are operating effectively.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

AGA member survey respondents have cybersecurity programs at varying degrees of maturity. Some have conducted risk assessment programs and have an advanced understanding of their risks and vulnerabilities, while other utilities are in the preliminary stages. The majority of publicly traded utilities are in the former group.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Yes, AGA member survey respondents have incident response programs to address and escalate threats and actual incidents. Internal monitoring and alerts received from ICS-CERT or from classified briefings can put the escalation process in motion.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Almost all states have existing privacy and civil liberties laws that provide coverage for personally identifiable information that may be affected by these practices.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

Most AGA member survey respondents are domestic natural gas utilities without international operations. If the Framework is appropriately designed, AGA members who have international operations do not see any international implications on global business or policy making.

11. How should any risks to privacy and civil liberties be managed?

Risks to privacy and civil liberties could be managed the way other risks are managed, by helping to ensure that appropriate controls are designed, implemented and monitored for effectiveness.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Employee education and awareness training should be a part of the framework. Given that the human element of any cybersecurity program progressively poses risk to the sector assets, periodic reminders are essential to the success of any program. In parallel with education and awareness is the inclusion of tabletop exercises and simulations.

AGA and its members are eager to continue to engage with NIST in the development of the Framework To Improve Critical Infrastructure Cybersecurity. One comment in closing refers back to the lengthy list of currently available standards, guidelines, best practices, and tools found in the response to question 7 in the first section of questions. We encourage NIST to utilize these existing works rather than develop additional standards.

Respectfully submitted,

James F. Linn, Jr.
Managing Director, Information Technology
American Gas Association
400 N. Capitol St, NW
Washington, DC 20001
202-824-7272
jlinn@aga.org