January 19, 2018

Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Mail Stop 2000
Gaithersburg, MD 20899

Re: **INGAA Comments on National Institute of Standards and Technology (NIST) Cybersecurity Framework Draft 2 of Version 1.1**

The Interstate Natural Gas Association of America ("INGAA") respectfully submits these comments in response to the public comment period for Draft 2 of the Cybersecurity Framework Version 1.1 ("Draft Framework"), which the National Institute of Standards and Technology ("NIST") published on its website on Tuesday, December 5, 2017.

INGAA is a trade organization that advocates regulatory and legislative positions of importance to the natural gas pipeline industry. INGAA's 27 members represent the majority of the interstate natural gas transmission pipeline companies in the United States. INGAA's members, which operate approximately 200,000 miles of pipelines, serve as an indispensable link between natural gas producers and consumers.

We appreciate NIST's continued efforts to support this cross-sector Cybersecurity Framework and the reduction of cybersecurity risks to critical infrastructure. This high-level Framework provides the appropriate mix of flexibility and specific risk management program components, providing private industry with effective guidance for their individual programs. Further, the collaborative approach to developing and revising the framework has served to strengthen the valuable and trusted partnership between NIST and private industry. INGAA commends NIST for its approach to working with private industry and soliciting feedback on these updates.

INGAA has reviewed the joint response filed by the American Gas Association and the Edison Electric Institute and would like to express its support for the comments contained within. In particular, INGAA would like to highlight the following:

The Framework should remain a voluntary, baseline tool

INGAA agrees that the framework should remain a voluntary, baseline tool for critical infrastructure. The framework serves as an effective baseline for reducing cybersecurity risks across all 16 critical infrastructure sectors. Any further sector-specific guidance should be coordinated through the Sector-Specific Agencies.

The updated Framework should continue to be informative and voluntary, but not prescriptive
As noted, the framework provides a useful baseline for cybersecurity risk management. INGAA appreciates efforts by NIST to remove the prescriptive and directive language included in Draft 1. INGAA agrees that the Framework should continue to be outcome and objective focused to remain technology neutral and preserve the voluntary approach.

Maintain harmony with existing rules and standards to sustain use of the Framework
INGAA agrees that the addition of supply-chain risk management provides a substantial improvement to the original framework. The framework should continue to be flexible enough to maintain harmony between various sector-specific rules and standards. For example, INGAA and its members also implement the *Transportation Security Administration Pipeline Security Guidelines*. Utilizing the NIST framework alongside appropriate sector-specific guidance and tools provides private industry with comprehensive guidance to assess, develop, and improve their cybersecurity capabilities and programs.

Again, INGAA greatly appreciates NIST's continued efforts to update and maintain the framework, while working closely with private industry to incorporate feedback. INGAA members look forward to the continued collaboration with NIST and our other Federal agency partners as we work together to strengthen critical infrastructure cybersecurity.

Sincerely,

Rebecca Massello
Director of Security, Reliability and Resilience
Interstate Natural Gas Association of America
20 F Street, NW, Suite 450
Washington, DC 20001
(202) 216-5933
rmassello@ingaa.org