TESTIMONY OF
REBECCA GAGLIOSTRO
DIRECTOR OF SECURITY, RELIABILITY AND RESILIENCE
INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA
BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY
AND THE
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE
PROTECTION AND INNOVATION
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES
REGARDING
SECURING U.S. SURFACE TRANSPORTATION FROM CYBER ATTACKS

February 26, 2019

Good morning Chairmen Correa and Richmond, Ranking Members Lesko and Katko, and members of the subcommittees. I am delighted to be here today to share our thoughts on cybersecurity in the pipeline industry. I am Rebecca Gagliostro, the Director of Security, Reliability and Resilience at the Interstate Natural Gas Association of America (INGAA). INGAA is a trade association that advocates regulatory and legislative positions of importance to the interstate natural gas pipeline industry in the United States. INGAA's 28 members operate approximately 200,000 miles of interstate natural gas pipelines that are analogous to the interstate highway system. Like the highways that are the arteries for so much of our nation's commerce, interstate natural gas pipelines are the indispensable link between U.S. natural gas producers and consumers. In my role at INGAA, I work directly with our members to ensure that our pipeline infrastructure remains resilient, safe, and secure.

Cybersecurity is a priority for the natural gas pipeline industry.

INGAA member companies work diligently to secure our nation's critical gas transmission infrastructure from cyber and physical security threats. The boards of directors and executive leadership of our member companies have identified cybersecurity as a top operational risk and take the management of this risk very seriously. Last year, in recognition of this priority, INGAA's Board of Directors stepped forward with its *Commitments to Pipeline Security*[1] statement, which enumerates specific actions that all of our member companies are taking to identify, protect, detect, respond to, and recover from security threats targeting our systems. In addition, the statement emphasizes our members' commitments to following the *Transportation Security Administration's (TSA's) Pipeline Security Guidelines* and the *National Institute of Standards and Technology's (NIST's) Cybersecurity Framework*, and to engaging in comprehensive information sharing across the industry and with our Federal partners. These are the foundations to building and maintaining strong pipeline security programs.

INGAA's commitments provide a high-level roadmap of what our member companies are doing to secure our infrastructure, as appropriate for public dissemination. In practice, our members' security programs are far more extensive than the information that may be conveyed by these

[1] *INGAA Commitments to Pipeline Security*, https://www.ingaa.org/File.aspx?id=34310&v=db10d1d2

commitments. It is our firm belief that we must be continually vigilant and entirely committed to the ongoing improvement of our security defenses because the adversaries seeking to harm infrastructure of all kinds, including natural gas pipelines, are nimble and the threats they pose are evolving.

Pipeline operators take a risk-management approach to addressing security threats. Industry security efforts seek to reduce the risk posed by a successful attack targeting our infrastructure. This risk-informed approach helps us prioritize our actions and allocate appropriate resources towards the highest priority. Pipeline operators utilize a variety of tools and resources, like the *NIST Cybersecurity Framework* and the *TSA Pipeline Security Guidelines*, to build well-rounded cybersecurity programs that effectively assess and manage the risks that we face. We recognize that cybersecurity risk management strategies must be comprehensive in nature and must implement measures to both reduce the likelihood of a successful attack and mitigate the impacts of a successful attack, should one occur. As such, pipeline operators assess their security programs using a variety of resources such as Federal assessment programs, self-assessments, peer reviews, and third-party vulnerability and penetration tests. Exercises and tabletops also play an important role in testing our security programs, sharing information with our peers about our security practices, and planning for how we will work across industry, interdependent sectors and with first responders during an incident.

A foundational element of a well-informed risk management program is comprehensive information sharing. This is a key point that deserves emphasis. Real-time, actionable information is vital to ensuring pipeline operators are equipped with the latest intelligence on threats, including known tactics, techniques, and mitigative measures. This, in turn, enables operators to evaluate their risks and tailor an approach that best fits the needs of their individual systems and environments. Strong information sharing already occurs today between INGAA member companies and other industry stakeholders through the work of our information sharing and analysis centers (ISACs), including the Downstream Natural Gas (DNG) ISAC and the Oil and Natural Gas (ONG) ISAC. However, this cannot be industry's responsibility alone. It is imperative that we also have a cooperative relationship with our government partners to facilitate rapid information sharing. It is worth emphasizing that the pipeline industry has a strong information sharing relationship with our partners at TSA and U.S. Department of Homeland Security (DHS). We would like to see this relationship of trust continue and develop, as we look towards these agencies to declassify threat intelligence and provide us with the timely, actionable information necessary to protect our systems and infrastructure.

The Transportation Security Administration pipeline security program is improving. The Aviation and Transportation Security Act (P.L. 107-71) ("ATSA") vested the Transportation Security Administration with authority over pipeline security. Pursuant to this authority, TSA offers guidance on expected practices and procedures necessary to secure the nation's critical pipeline infrastructure. TSA offers several programs, tools, and products to assist pipeline operators with protecting their infrastructure, including Critical Facility Security Reviews, Corporate Security Reviews, Pipeline Cybersecurity Assessments, Smart Practices, I-STEP, Security Awareness Training Videos, and the International Pipeline Security Forum.

TSA acknowledges that there remains room for improvement in its pipeline security program. The agency has accepted the recommendations for improving the management of its pipeline security program that were made by the Government Accountability Office and is in the process of implementing them. INGAA strongly believes that if followed, these recommendations will help to make a stronger and more robust program.

Following the tragic events of September 11, 2001, TSA's security program was rooted in the physical security threats targeting our critical infrastructure. As acknowledged in a recent statement by Director of National Intelligence Dan Coats, sophisticated nation-state backed cybersecurity capabilities present a real threat to our critical infrastructure. These threats have led to increased emphasis by TSA and our sector on protecting pipeline infrastructure from cybersecurity threats. It is important to stress that these threats are faced by all critical infrastructure and not just natural gas pipelines. The increasing interdependence across the segments of our nation's critical infrastructure means that we must work together across industry and government to protect ourselves against these threats.

The work that TSA and DHS are doing through the National Risk Management Center (NRMC) is a very positive step toward the end goal of protecting the nation from cybersecurity threats. These agencies are working together to understand how sophisticated, nation-state threat actors seek to identify ways to harm all U.S. critical infrastructure. We believe this approach is significant because these threats cannot be analyzed effectively in isolation. *All* critical infrastructure is being targeted; therefore, we must identify the best ways to work *together* to protect our national security.

In October, these agencies announced the Pipeline Cybersecurity Assessment Initiative, which is working to conduct comprehensive cybersecurity assessments of natural gas infrastructure to better understand the unique risks faced by our infrastructure as well as to identify how best to protect it. In addition to having a recognized baseline of practices, assessments are critical to providing assurance that these programs are working. TSA has already piloted one INGAA member assessment in 2018, and INGAA members continue to volunteer to participate in these new assessments in 2019.

Next steps for building upon progress to secure pipeline infrastructure.
INGAA believes that progress has been made in securing our pipeline infrastructure and that the focus should be on continuing to improve TSA's pipeline security program. Threat actors regularly develop and refine their tactics, and we must do the same. The increased coordination between TSA and DHS's Cybersecurity and Infrastructure Security Agency (CISA) through the NRMC is an appropriate response to the enhanced need for cybersecurity expertise to support industry's efforts to protect our critical infrastructure against these growing threats. We understand TSA has embraced GAO's recommendations as a roadmap for improving its pipeline security program and is already taking steps to respond to them.

INGAA and its member companies will continue to support TSA's efforts. This includes volunteering for assessments, sharing information about indicators of compromise and about how member companies are securing their infrastructure, and participating in cross-sector exercises so we can better determine how the different segments of critical infrastructure must work together.

The growing threat of nation-state backed attacks requires a coordinated and comprehensive approach across all critical infrastructure and across all Federal agencies supporting national security. INGAA believes that TSA’s ongoing work with the NRMC and CISA is bridging that gap. We urge Congress to support TSA’s efforts to improve its program and to provide the necessary guidance and funding for additional program management staffing and cybersecurity expertise that can work directly with the NRMC and support the new Pipeline Cybersecurity Assessment Initiative. INGAA believes that this supplement to efforts already underway will help make TSA successful in its mission to protect the nation’s pipeline infrastructure.