Interstate Natural Gas Association of America

July 10, 2024

To: Natural Gas Pipeline Hardware, Software, and Industrial Control System Vendors & Suppliers

Re: Secure By Design Pledge & Supply Chain Cybersecurity Principles

To whom it may concern,

Members of the Interstate Natural Gas Association of America (INGAA) write today to urge all hardware, software, and industrial control systems technology and equipment providers to consider and ultimately take the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE) pledges to manufacture their products securely.

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

INGAA members routinely defend against network intrusion attempts by sophisticated adversaries and, consequently, are subject to the first cybersecurity requirements for the subsector's critical infrastructure through the Transportation Security Administration (TSA). The outcome-based approach that TSA has implemented with pipelines is a regulatory framework that allows the owners of the risk to determine the best means to achieve the desired security outcome. However, this is only half of the battle; every company is dependent on technology built securely to deploy in pipeline systems. Without secure devices, regulation is null, security is meaningless, and U.S. critical infrastructure remains vulnerable to targeted attacks.

To that end, CISA's efforts to weld together a threat awareness ecosystem within Secure by Design and the Joint Cyber Defense Collaborative (JCDC) sends appropriate messages that broad private-public partnerships can reduce critical infrastructure cybersecurity risks, including to pipeline systems. Notably, the prioritization of threat-informed product development practices that are at the core of Secure by Design are of great value to critical infrastructure operators. Owners and operators have an opportunity to add another layer of defense and efficacy by leveraging Secure by Design vendors in their supply and procurement processes, and we believe the concept should become a powerful demand-side program.

Similarly, DOE's Supply Chain Cybersecurity Principles align best practices and identify opportunities for the industrial control system vendor community to strengthen the manufacturing supply chain of key technologies that manage and operate our pipeline systems. These Principles, informed by the subject matter expertise of Idaho National Laboratory (INL), are a foundational step toward securing critical

forms of equipment and technology before they can be exploited. In particular, DOE's proactive model of vendor-to-operator engagement throughout the lifecycle of the product is essential for operator risk management.

Collectively, these efforts rightly signal that security is a shared responsibility among manufacturers, service providers, and operators. INGAA members strongly endorse the Secure by Design and Supply Chain Cybersecurity Principles concepts as developed by CISA and DOE and the vendors pledging to implement these into their product development. We applaud those organizations who have already made the commitment and taken steps to engineer their products securely each step of the way. We understand the critical need for secure devices and the opportunity for private-public partnerships to help raise the security posture of the sector through Secure by Design and supply chain secure technology. We are ardent supporters of a vendor-level partnership, and our procurement practices will continue to evolve to reflect the need for secure technologies.

INGAA members take the security of their assets seriously and encourage all technology and equipment providers, particularly those with a strong market share in critical infrastructure operations, to take the CISA and DOE pledges to manufacture their products securely throughout the entire systems' engineering lifecycle. Additionally, our members urge the highest levels of vendor organizations to engage with our government partners to ensure their products are, and remain, secure.

Sincerely,

Members of the Interstate Natural Gas Association of America

CC: Cybersecurity & Infrastructure Security Agency
Department of Energy
Transportation Security Administration