June 24, 2022

Scott Gorton
Executive Director, Surface Policy Division
Policy, Plans & Engagement
Transportation Security Administration
Washington, DC

Dear Executive Director Gorton,

Thank you for the opportunity to provide comments on draft Security Directive Pipeline-2021-02C. Pipeline cybersecurity mitigation actions, contingency planning, and testing are all vital activities for protecting our nation's most critical gas and liquid pipeline systems.

The pipeline industry shares the goals of the Transportation Security Administration (TSA) to reduce the vulnerability of critical pipeline operations and facilities to cybersecurity threats through implementation of layered cybersecurity measures that provide defense-in-depth.

We commend Administrator Pekoske for his vision of an outcome-based program that is effective across the broad range of pipeline systems and innovative in adapting to evolving threats. We are grateful for the opportunities TSA provided this spring for pipeline operator subject matter experts to share their pipeline operations-specific cybersecurity knowledge and insights with TSA.

Covered pipeline owners and operators, as well as representative trade associations, are submitting comments. Many of those comments address individual technical issues throughout the draft. We offer these joint comments on several of the broader, process-oriented issues the draft presents. Thank you in advance for your consideration of these issues.

Short Submission Deadline

Section II(B)(1) requires owner/operators to submit a Cybersecurity Implementation Plan (CIP) for TSA approval within 60 days. There is universal consensus that this time period is insufficient. Effective CIPs will require customization to an owner/operator's system and the conditions they face. TSA is requiring CIPS to provide all the information required by Sections III.A. through III.E. and describe in detail the owner/operator's defense-in-depth plan,

including physical and logical security controls, for meeting each of the requirements in Sections III.A through III.E. To meet this expectation, we recommend TSA adopt a development period in the 120 to 180-day range.

TSA Pre-Approval Delays

TSA proposes owner/operators to submit a CIP to TSA for approval and the CIP is not effective until TSA grants that approval. Industry has grave concerns about TSA's ability to review and approve nearly 100 CIPs in a timely manner. Indeed, a driving rational for SD-02C are the challenges TSA faced reviewing and approving alternative measure proposals. We understand TSA will request and receive additional resources to meet this obligation. However, the challenge TSA will create for itself in requiring TSA pre-approval of submitted CIPs before they become effective are orders of magnitude larger than the current SD-2B system. We fear delays processing CIPs will range long into the future, a situation which does not benefit TSA nor national security.

Instead, we recommend TSA adopt the proven approaches of the U.S. Pipeline and Hazardous Materials Safety Administration (PHMSA) and the Canada Energy Regulator (CER) of requiring owner/operators to develop and implement and follow plans and systems within a certain time period. To provide for pipeline safety within high consequence areas, PHMSA in 49 CFR 195.452 required pipeline operators to not only develop within 1 year a written integrity management program that addresses the risks on each covered segment of pipeline (b)(1), but also implement and follow the program (b)(5). Similarly, conditions issued in orders and certificates issued pursuant to section 214 and section 183 of the *Canadian Energy Regulator Act* require an officer of the company within a defined time to certify completion of a pipeline construction project and that the project was constructed in compliance with all applicable conditions.

Accountability is maintained through government audit and inspection programs. Both PHMSA and the Canadian government audit and inspect pipeline operators. We expect TSA to implement a robust audit and inspection program to confirm compliance with TSA SDs. We understand TSA's desire to avoid any gaps in coverage during SD-02C CIP development. We support TSA keeping SD-02B requirements in place until SD-02C plans are developed and implemented. However, to avoid inevitable severe delays in reaching that point, we recommend TSA adopt a company certification and government audit/inspection approach for SD-02C CIP development and implementation.

Delivery of Documentation to Establish Compliance

TSA proposes to require owner/operators to provide TSA with documentation to establish compliance with SD-02C. TSA provides a lengthy list of type of documentation TSA expects. We appreciate the protections of sensitive security information TSA will impose. However, we are concerned TSA does not appreciate the incredibly massive volume of data and materials TSA request may entail. For example, 24-hour capture network traffic of (C)(2)(c) could entail terabytes of data. All of these documents could require petabytes of storage. Policy, procedural

and other documents that merely informed development of the CIP as required by (C)(2)(g) could also prove extremely extensive.

We do not question TSA's desire and need to review documentation establishing compliance with SD-02C. Indeed, PHMSA inspection of operator compliance with federal pipeline safety requirements involves lengthy and detailed document review. However, PHMSA manages this process to the benefit of both inspectors and operators by viewing documents virtually when offsite, requesting selected documents in advance of scheduled inspections, and spot-checking policies, procedures and documentation of compliance during in-person inspections. We urge TSA to consider these practical solutions to manage their compliance program.

Barriers to Improvement Actions

Section VI(B) appears to require operators obtain approval from TSA to not only change its CIP, but also policies, procedures or measures related to the CIP. We fear this requirement will impede operators' desires to make updates or improvements to its security programs. Pipeline operators believe strongly in the plan-do-check-adjust approach of safety management systems (SMS). Pipeline operators with SMS programs seek continuous improvement of their performance by evaluating their programs and making adjustments based on their reviews. This type of approach is especially vital for effective cybersecurity programs which must often evolve and change, sometimes on short notice and without delay. An overly broad TSA approval requirement for amendments to program documents will slow and potentially impede improvement efforts. Additionally, we expect a robust TSA audit and inspection program will ensure changes made to owner/operator CIPs are effective. Similar to development and implementation of CIPs, we recommend TSA adopt a company certification and government audit/inspection approach for SD-02C CIP amendments.