JAMES LANKFORD
OKLAHOMA

COMMITTEES:
FINANCE
ENERGY AND NATURAL RESOURCES
INDIAN AFFAIRS
ETHICS
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS

United States Senate

WASHINGTON, DC OFFICE:
316 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5754

OKLAHOMA CITY OFFICE:
1015 NORTH BROADWAY AVENUE, SUITE 310
OKLAHOMA CITY, OK 73102
(405) 231-4941

TULSA OFFICE:
401 SOUTH BOSTON AVENUE, SUITE 2150
TULSA, OK 74103
(918) 581-7651

July 9, 2021

The Honorable Alejandro Mayorkas
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Mayorkas:

As a member of the Senate Homeland Security and Governmental Affairs Committee, I appreciate the Department's ongoing work to enhance pipeline sector cybersecurity programs and oversight. My state of Oklahoma is a leader in the energy sector and knows the importance of delivering traditional fuel for national security. I write to encourage you to ensure that new programs and requirements currently under consideration are 1) properly prioritized and phased-in; 2) risk-based and nimble; and 3) where appropriate, developed using public notice-and-comment procedures, all with the goal of ensuring that energy continues to flow reliably, affordably, and securely to families and businesses across our nation.

As demonstrated by the ransomware attack on the Colonial Pipeline Company last month and by other recent attacks on both public and private networks, enhancing America's critical infrastructure cybersecurity, including pipeline cybersecurity, is of vital national importance. I recognize that the administration is currently pursuing several new pipeline cybersecurity initiatives.

On May 27th, the Transportation Security Administration (TSA) exercised its emergency authority to require critical pipeline operators to take a number of actions, including: reporting cyber intrusions to the Cybersecurity and Infrastructure Security Agency (CISA); conducting a review of their company's cybersecurity protections and reporting the results to TSA and CISA; and establishing dedicated cybersecurity coordinators to enhance two-way communication between pipeline operators and the Department.[1]

When announcing this emergency directive, and during a hearing before subcommittees of the House Homeland Security Committee, the Department indicated that it is considering further "follow-on mandatory measures" regarding pipeline cybersecurity, including mandating certain specific mitigation measures.[2] In addition to these TSA directives, the National Security Council has indicated that it is working on a separate initiative "to enhance the security of critical infrastructure systems and improve visibility across their operational control systems," which will include natural gas pipelines.[3]

[1] *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators*, DEP'T OF HOMELAND SEC. (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[2] *Id.; Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack*, 117th Cong. (2021) (statement of Sonya Proctor, Transportation Security Administration).

[3] *Press Briefing by Press Secretary Jen Psaki, Homeland Security Advisor and Deputy National Security Advisor Dr. Elizabeth Sherwood-Randall, and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger*, THE WHITE HOUSE (May 10, 2021), https://www.whitehouse.gov/briefing-room/press-

Given these potentially concurrent efforts, it is critically important that the administration's new pipeline cybersecurity initiatives are appropriately prioritized and phased-in. Government and industry should focus on the most productive and pressing activities first. Attempting to simultaneously implement numerous new cybersecurity requirements without sufficient lead time can cause operational disruptions and energy reliability challenges, which clearly would be counter to the goals of the Department's initiatives, and divert both agency and private sector resources from the most important activities.

Additionally, new initiatives should be nimble and risk-based, allowing pipeline operators to implement programs that are tailored to their specific systems and that leverage the full range of cybersecurity technologies available today, while avoiding locking-in technologies that may become outdated in the future.

Finally, although Congress has provided TSA emergency procedures that enable the agency to implement new requirements without providing advanced notice or opportunity for public comment,[4] that authority should be reserved for truly urgent actions, and most regulatory proposals should still be subject to Administrative Procedures Act requirements. Given TSA's actions are the first in setting cybersecurity requirements for pipelines, a transparent and open process is critical to ensuring a balanced approach.

Thank you for your attention to my recommendations, and I welcome any conversation to ensure a measured approach is taken to enhance critical infrastructure cybersecurity. Please let me know how I can be of further assistance.

In God We Trust,

James Lankford
United States Senator

Cc:
The Honorable Chris Inglis, United States National Cyber Director
The Honorable Jake Sullivan, United States National Security Advisor

briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/.

[4] 49 U.S.C. § 114(l)(2)(A).