

United States Senate

WASHINGTON, DC

October 28, 2021

The Honorable Joseph V. Cuffari
Inspector General
Department of Homeland Security
Office of the Inspector General
Washington, D.C. 20528-0305

Dear Mr. Cuffari:

We write to request you review the process by which the Transportation Security Administration (TSA) has developed and issued several emergency security directives this year, including recently issued and announced cybersecurity directives developed in consultation with the Cybersecurity and Infrastructure Security Agency (CISA).

Our critical infrastructure must be secured and protected against cyberattacks. However, securing critical infrastructure requires a collaborative approach with the experts in these industries—the people who operate this critical infrastructure and who are charged with implementing these directives. We believe that care must be taken to avoid unnecessarily burdensome requirements that shift resources away from responding to cyberattacks to regulatory compliance. Unfortunately, we have received reports that TSA and CISA failed to give adequate consideration to feedback from stakeholders and subject matter experts who work in these fields and that the requirements are too inflexible. We are also troubled that TSA and the DHS Office of Legislative Affairs (DHS OLA) refused to provide copies of the draft directives to Congress, including the Chairs and Ranking Members of its congressional oversight committees, despite having shared copies with the pipeline industry.

The TSA Administrator has the statutory authority to issue security regulations in the transportation sector. Under a related authority, which had never before been exercised with the pipeline sector, the Administrator may issue emergency security regulations or directives without notice and comment if the Administrator determines that it “must be issued immediately in order to protect transportation security.”¹ At least until earlier this year, TSA had worked in close coordination with industry stakeholders to develop practical security guidelines and policies.²

We are concerned that the recently issued security directives appear to depart from TSA’s historically collaborative relationship with industry experts. On May 27, 2021, in response to the Colonial Pipeline ransomware attack, TSA Administrator David Pekoske exercised the emergency security directive authority and issued TSA’s first ever pipeline-focused security directive (SD-01).³ On July 20th, TSA issued a second security directive to the pipeline industry

¹ 49 U.S.C § 114 (l)(2)(A).

² TRANSP. SEC. ADMIN, U.S. DEP’T OF HOMELAND SEC., PIPELINE SECURITY GUIDELINES (2018), *available at* https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

³ Ratification of Security Directive, 86 Fed. Reg. 38209 (Jul. 20, 2021); Press Release, U.S. Dep’t of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27,

entitled, “Security Directive Pipeline-2021-02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing” (SD-02).⁴ In response, on August 24, 2021, associations representing more than 2,700 companies in the oil and natural gas subsector sent a letter to TSA Administrator Pekoske warning of inadequate consultation and that the resulting security directives could have “operational safety and reliability” impacts.⁵

On October 6th, Secretary Mayorkas announced TSA would issue additional security directives requiring railroad and airport operators to improve their cybersecurity practices.⁶ Public reports again indicate that TSA provided very little time for industry feedback.⁷

Another area of concern is that TSA and the DHS OLA also refused to provide copies of the draft directives to Congress, including the Chairs and Ranking Members of its congressional oversight committees, despite having shared copies of the drafts with the pipeline industry. In a briefing with Senate staff on July 15, 2021, TSA officials explained they would not be providing a draft of SD-02 to Senate staff because it was pre-decisional and therefore deliberative.⁸ This argument appears to misapprehend the function and limits of the deliberative process privilege, which is not a bar to disclosure, especially not to Congress, and in any event is generally considered waived once an agency has “officially acknowledged” the record by prior disclosure outside the Government, as here.⁹

We agree that critical infrastructure must be protected against cyber-attacks, particularly in the wake of the Colonial Pipeline ransomware attack, but the process by which TSA has issued these directives raises concerns. To address these concerns, we request that you review TSA’s development and issuance of emergency security directives this year. Specifically, we request that you examine the following with regard to each emergency security directive or emergency amendment related to cybersecurity issued this year:

1. The basis for the directive or amendment and, in each case, the basis for employing the emergency authority under section 114(1)(2) of title 49, United States Code, to issue those directives without full notice and comment, including:
 - a. Any consultation with the Office of the Secretary of Homeland Security or the Executive Office of the President;

2021), <https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>.

⁴ Press Release, U.S. Dep’t of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (Jul. 20, 2021), <https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>.

⁵ Letter from Pipeline Trade Associations to TSA Administrator David P. Pekoske (Aug. 24, 2021) (enclosed).

⁶ Press Release, U.S. Dep’t of Homeland Sec., Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit (Oct. 6, 2021), <https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit>.

⁷ E.g., Oriana Pawlyk, *Freight rail blasts TSA cybersecurity proposal as redundant*, Politico (Oct. 6, 2021), <https://subscriber.politicopro.com/article/2021/10/freight-rail-blasts-tsa-cybersecurity-proposal-as-redundant-3991607>.

⁸ Briefing with HSGAC Staff (Jul. 15, 2021) (notes on file with Committee).

⁹ See, e.g., *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (1990).

- b. TSA's identification of additional threats to pipeline critical infrastructure, rail transit systems, and the aviation sector; and
 - c. The timing of the directives and announcements of the directives including those announced on October 6;
2. The consultation process with stakeholders in each case, including industry, other agencies, and Congress, which should examine:
 - a. The timeline for affected industries to provide feedback;
 - b. The extent to which TSA modified draft security directives to address industry comments or concerns; and
 - c. The Federal agencies who contributed to the development of these security directives and their involvement;
 3. The basis for designating of all or parts of the draft and final security directives and related documents as Sensitive Security Information (SSI) and the non-designation of the final SD-01 as SSI including:
 - a. Whether the SSI designation was used to restrict access for any reason other than those reasons authorized by law;
 - b. The basis for designating information as SSI in a draft but not a final security directive; and
 - c. The specific information designated as SSI in each draft or final security directive and why such a designation was made; and
 4. The basis for withholding the draft directives from Congress.

We request that you review this matter and submit a report to us within 120 days. In the interim, we request that you provide us with monthly updates. Thank you for your prompt attention to this important request.

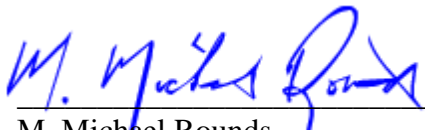
Sincerely,



Rob Portman
Ranking Member
Committee on Homeland Security &
Governmental Affairs



James Lankford
Ranking Member
Subcommittee on Government Operations
& Border Management, Committee on
Homeland Security & Governmental Affairs



M. Michael Rounds
United States Senator

Enclosure



August 24, 2021

The Honorable David P. Pecoske
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598-6020

Administrator Pecoske,

The included pipeline trade associations, AFPM, AGA, AOPL, API, APGA, INGAA, and GPA Midstream appreciate the opportunity to provide feedback on the recent Security Directive 2021-02, issued on July 19, 2021 (Directive). These trade associations represent almost all aspects of U.S energy pipeline operations that serve customers reliably across North America. The associations' members represent refineries and petrochemical operators -- through which pipelines receive and distribute products, regional and local natural gas distribution pipelines, liquids pipelines, integrated and midstream natural gas and oil companies, operators of municipal natural gas systems, natural gas transmission pipelines, and natural gas product pipelines and processors. Across the industry, our members all share the same concerns with the implementation of Security Directive 2021-02 and the process with which it was developed. For nearly two decades, we have worked along-side TSA in a structured oversight model applying risk-based methodology that properly balanced pipeline security with operational reliability and safety. We understand the ongoing situation presented by ransomware and other cyber threats to critical infrastructure and are committed to working with TSA to continue sound pipeline security practices and policies.

Open communication, process transparency, and timely engagement with the industry have been hallmarks of the TSA pipeline security program. Concerningly, these fundamental elements of a strong security partnership were not fully realized during the process used to develop the Directive. We wish to reemphasize the need for TSA to work efficiently with affected companies on successful Directive implementation, especially now that compliance deadlines are approaching. We encourage TSA and its technical experts to work closely with industry experts to ensure mutual understanding of how requirements in the Directive could impact operational reliability.

While we appreciate that TSA published an initial list of frequently asked questions (FAQs) focused on administrative matters, there remain several unanswered technical questions submitted by the associations and our members to which TSA guidance is critical for compliance. These unanswered questions have left operators with significant uncertainty about what is required for compliance. We urge TSA to release the technical FAQs in a timelier manner—TSA's timeline to responding to questions should be consistent with the rapid deadlines established under the Directive. We also ask TSA to apply learnings from the recent Directive development process to improve the agency's procedures for



obtaining stakeholder input on future pipeline security initiatives and avoid recreating the implementation challenges and uncertainty our members are now experiencing.

Operational reliability and safety are extremely important to the pipeline industry. The Directive's potential to cause operational disruptions or threaten safe operations remains a concern of affected pipeline operators. Our pipeline operators have expert knowledge regarding their assets, how they are managed to meet customer needs, and how to comply with the various state and federal regulations under which they are required to operate. As the Directive was developed, industry conveyed highly probable operational safety and reliability concerns that could arise by imposing prescriptive cyber requirements and untenable timelines without specific understanding of a company's existing cybersecurity protections and operations. We appreciate that TSA addressed some of our recommendations and responded to our feedback. Regrettably, significant concerns remain. The broad scope and prescriptive nature of the Directive create potential conflicts with TSA pipeline Security Guidelines and with existing cybersecurity and safety regulations from other federal government entities. The prescribed implementation schedule creates safety and reliability concerns. We urge TSA to work closely and quickly with operators on Directive implementation to ensure affected pipelines do not have to choose between complying with the Directive and ensuring continued safety and reliable operations.

The Directive allows operators flexibility to submit alternative compliance options to TSA for consideration, and TSA has stated it will respond promptly to these submissions. We recognize TSA believes operator concerns may be addressed through this alternative submittal option. However, the usability of this option is limited without further clarity on TSA's anticipated criteria and timelines for review of alternative proposals relative to the Directive's deadlines, what recourse operators have if TSA disagrees with proposed alternative compliance options, and how TSA will address scenarios where an operator determines that extensive equipment retrofits will take longer time periods than envisioned by TSA. Furthermore, TSA should ensure operators are not penalized for awaiting TSA's clarification of these issues and approval of alternative proposals as the Directive's deadlines approach.

Pipeline operators also face challenges applying the Directive in the context of broader corporate structures, given that cybersecurity for some pipeline operations is managed across individual companies and countries as part of enterprise-level cybersecurity and information technology systems that also cover non-pipeline operations. As the Directive is currently written, and without clarity from TSA, some operators are in the position of guessing what nonoperational networks (e.g., finance, HR, etc.) are impacted by the Directive and may be applying prescriptive measures that divert resources while not addressing the actual risks to pipeline operations. We urge TSA to provide more clarity on the scope, so that operators can make more sound determinations of what is necessary to avoid disrupting operations or threatening pipeline safety.

We also urge TSA to reconsider its process for implementing pipeline security initiatives in the future to ensure better input on the compatibility of proposed security requirements with pipeline operational technology. It is important TSA make timely updates to its pipeline security policies to keep up with



evolving threats. At the same time, it is equally important TSA's process does not sacrifice input from the regulated industry for the sake of speed. TSA's authorizing statute¹ and the Administrative Procedures Act require that the agency use formal notice-and-comment rulemaking as the primary vehicle for issuing new requirements. In this case, we believe the robust stakeholder input and advisory committee review provided by a notice-and-comment rulemaking would have resolved many of the substantive challenges created by the current Directive text and promoted stronger public-private partnership for pipeline security. We acknowledge that TSA may wish to protect certain aspects of its proposed requirements as Sensitive Security Information and note that procedures other than formal notice-and-comment can also be successful in soliciting and incorporating necessary input on a timely basis.

Our associations are also concerned that, as you testified to the Senate Commerce Committee on July 27, 2021, there is additional threat information driving the urgency of the Directive and the timelines that have been set. This threat intelligence has not been shared with potentially affected companies. Pipeline operators are best positioned to design mitigations to defend their systems against new threats based on their risk-based security programs. They are unable to effectively prepare for threats about which they have not been briefed. While we do appreciate the recent offer of a Secret level briefing to a limited group of associations within the Beltway, we again highlight the need for TSA, and the broader intelligence community, to ensure they are sharing the most timely and relevant information directly with the potentially impacted operators. We urge TSA, and other agencies that have threat information relevant to pipelines, to brief all potentially affected companies as soon as possible to ensure they can appropriately defend against current threats. We also encourage TSA to work with the broader intelligence community (IC) to provide regularly scheduled briefings to pipeline industry experts to ensure operators are appropriately informed about the evolving threats to their systems. TSA should also work with the IC to provide as much timely, unclassified information as possible to operators to ensure it is actionable and can be disseminated to operators who do not possess security clearances.

Listed below is a summary of our requests.

- TSA and its technical experts should work closely and quickly with industry experts to ensure mutual understanding of how requirements in the Directive could impact operational safety and reliability.
- TSA should release the technical FAQs immediately.
- TSA should provide clarity on anticipated criteria and timelines for review of alternative proposals, including addressing operator recourse if TSA disagrees with the alternative proposal and how TSA will address supply chain limitations.
- TSA should ensure operators are not penalized for awaiting TSA's review of alternative proposals.

¹ 49 U.S.C. § 114(l)(2)(A).



- TSA should provide more clarity on the Directive's scope so that operators can make more sound determinations of what is necessary to avoid disrupting operations or threatening pipeline safety.
- TSA should reconsider its process for implementing pipeline security initiatives in the future to ensure better input on the compatibility of proposed security requirements with pipeline operational technology.
- TSA and pertinent government intelligence community should brief all potentially affected pipelines on relevant cybersecurity threat intelligence as soon as possible.

The associations and our members are committed to supporting efforts to build pipeline cyber security capability, and we look forward to further discussing our concerns and potential solutions to ensure the Directive implementation can be successful.