OFFICE OF INSPECTOR GENERAL

Better TSA Tracking and Follow-up for the 2021 Security Directives Implementation Should Strengthen Pipeline Cybersecurity (REDACTED)

Homeland Security

September 26, 2023

OIG-23-57

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

September 26, 2023

MEMORANDUM FOR: The Honorable David Pekoske
                    Administrator
                    Transportation Security Administration

FROM: Joseph V. Cuffari, Ph.D.   JOSEPH V CUFFARI   Digitally signed by JOSEPH V CUFFARI
                    Inspector General   Date: 2023.09.22 09:00:51 -04'00'

SUBJECT: *Better TSA Tracking and Follow-up for the 2021 Security Directives Implementation Should Strengthen Pipeline Cybersecurity – ~~Sensitive Security Information~~*

For your action is our final report, *Better TSA Tracking and Follow-up for the 2021 Security Directives Implementation Should Strengthen Pipeline Cybersecurity – ~~Sensitive Security Information~~*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving TSA's ability to ensure pipeline operators implement the 2021 cybersecurity directives. Your office concurred with all three recommendations. Based on information provided in your response to the draft report, we consider all three recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act,* we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS
Better TSA Tracking and Follow-up for the 2021 Security Directives Implementation Should Strengthen Pipeline Cybersecurity

September 26, 2023

Why We Did This Audit

TSA issued two pipeline security directives in FY 2021 following the Colonial Pipeline ransomware attack. We conducted this audit to determine whether TSA's 2021 security directives addressed cyber threats and stakeholder concerns and strengthened pipeline security.

What We Recommend

We are making three recommendations to improve TSA's ability to ensure pipeline operators implement the 2021 security directives.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at
DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Transportation Security Administration's (TSA) fiscal year 2021 pipeline security directives, if implemented, should strengthen pipeline operators' posture against cyber threats. TSA considered and partially addressed stakeholder feedback when drafting these two directives. However, TSA did not ensure all pipeline operators timely adhered to security requirements contained in the directives. For example, ■ of 97 critical pipeline operators did not meet one or more requirements in *Security Directive Pipeline–2021–02 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD-02). Additionally, TSA used action plans and warning notices to bring pipeline operators into compliance with SD-02, but TSA could not easily provide related information, such as which SD-02 requirements remained unresolved.

TSA also did not follow up and track the pipeline operators' assessments of the effectiveness of their cybersecurity practices. This occurred because TSA does not have standard operating procedures or a formal system to track and follow up on pipeline operators' implementation of the security directives. Without additional oversight, TSA cannot ensure full implementation of security directives, which can leave pipelines vulnerable to cyber attacks.

TSA Response

TSA concurred with all three of our recommendations, which we consider open and resolved.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Background

The 2021 Colonial Pipeline data breach and ransomware attack illustrated vulnerabilities in private industry and government networks and systems to cyber attacks. The pipeline operator decided to temporarily discontinue operations for several days due to the attack, resulting in fuel shortages and increased fuel prices.

Following the attack on Colonial Pipeline, the Transportation Security Administration (TSA)[1] in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), the operational lead for Federal cybersecurity, issued new cybersecurity requirements for pipeline operators via two security directives.[2] This was the first time TSA had used its authority to issue security directives under 49 U.S.C. § 114(l)(2)(A) for the pipeline industry. These security directives apply to critical pipelines, as determined by TSA. As of May 2021, TSA determined that 97 pipeline operators were critical and must comply with the security directives.

- First, on May 26, 2021, TSA issued *Security Directive Pipeline–2021–01 Enhancing Pipeline Cybersecurity* (SD-01). SD-01's main purpose was to require critical pipeline operators (i.e., those operating pipelines that TSA has designated as critical that transport hazardous liquids and natural gas) to designate a cybersecurity coordinator, report cybersecurity incidents, and conduct a vulnerability assessment.

- Second, on July 19, 2021, TSA issued *Security Directive Pipeline–2021– 02 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD-02),[3] which required owners and operators of TSA-

---

[1] Pursuant to 49 U.S.C. § 114(d), TSA is responsible for security in all modes of transportation, including but not limited to civil aviation.

[2] To address cybersecurity vulnerabilities affecting rail and other surface transportation industries, TSA issued two additional security directives, *Security Directive 1580-21-01 Enhancing Rail Cybersecurity* (SD-03) and *Security Directive 1582-21-01 Enhancing Public Transportation and Passenger Railroad Cybersecurity* (SD-04). These additional directives were not within the scope of our audit.

[3] TSA originally issued *Security Directive Pipeline–2021–02 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD-02) with a Sensitive Security Information designation to prevent bad actors from identifying cybersecurity vulnerabilities that had been discussed in the directive. On June 6, 2022, TSA determined that the security directive no

designated critical pipelines to implement additional and immediately needed cybersecurity measures to prevent disruption and degradation to their infrastructure in response to an ongoing threat.

In response to these directives, pipeline operators reported concerns with the requirements put forth in the security directives, including reporting timeframes and overly general terms.[4] TSA has updated the requirements of these security directives several times to include changes to certain definitions and timelines.[5]

We conducted this audit to determine whether TSA's 2021 security directives addressed cyber threats and stakeholder concerns and strengthened pipeline security. We focused our audit on the drafting, issuance, and implementation of SD-01 and SD-02.

Results of Audit

TSA's 2021 Pipeline Security Directives, if Implemented, Should Strengthen Pipeline Operators' Posture Against Cyber Threats

TSA's FY 2021 pipeline security directives, if implemented, should strengthen pipeline operators' posture against cyber threats. Following the attack on the Colonial Pipeline, TSA developed security directives SD-01 and SD-02 in consultation with CISA, the United States Coast Guard, the U.S. Department of Energy, and the Pipeline and Hazardous Materials Safety Administration of the U.S. Department of Transportation. SD-01 required critical pipeline operators to:

- designate a cybersecurity coordinator within 7 days;

---

longer contained sensitive information and the Sensitive Security Information designation was removed.

[4] Eric Geller, *'TSA has screwed this up': Pipeline cyber rules hitting major hurdles,* Politico (Mar. 17, 2022), https://www.politico.com/news/2022/03/17/tsa-has-screwed-this-up-pipeline-cyber-rules-hitting-major-hurdles-00017893 and Marco Ayala, *Pipeline Cybersecurity Implementation Plan for TSA Security Directive* (Pipeline & Gas Journal, October 2022, Volume 249, No. 10), https://pgjonline.com/magazine/2022/october-2022-vol-249-no-10/features/pipeline-cybersecurity-implementation-plan-for-tsa-security-directive.

[5] As of July 27, 2023, the active security directives are SD-01C (effective May 29, 2023) and SD-02D (effective July 27, 2023).

- report significant cybersecurity incidents to CISA within 12 hours; and
- assess their current cybersecurity posture, identify any gaps, develop a remediation plan, and report these items to TSA and CISA within 30 days.

SD-02 required pipeline operators to:

- implement critically important mitigation measures to reduce the risk of compromise from a cyber attack;
- develop a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption should information and operational technology systems be affected by a cybersecurity incident; and
- test the effectiveness of cybersecurity practices through a cybersecurity architecture design review (ADR).

TSA based SD-01's cybersecurity vulnerability assessment requirements on security measures from its *Pipeline Security Guidelines March 2018 (with Change 1 (April 2021)),* which were organized according to the National Institute of Standards and Technology (NIST) cybersecurity framework. NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, Federal agencies, and the broader public. Additionally, SD-02 indicated that implementation of the security directives by their established deadlines was necessary to protect transportation security.

TSA Considered Stakeholder Feedback When Drafting Pipeline Security Directives

Security directives issued under 49 U.S.C. § 114(l)(2)(A) are subject to review by the Transportation Security Oversight Board (TSOB) composed of the following members or their designees: the Secretary of Homeland Security, the Secretary of Transportation, the Attorney General, the Secretary of Defense, the Secretary of the Treasury, the Director of National Intelligence, and a presidential appointee representing the National Security Council. The TSOB is required to review and ratify or disapprove any security directive within 30 days of issuance.[6] Security directives issued under 49 U.S.C. § 114(l)(2)(A) do not require public notice or a comment period.

The TSOB reviewed and ratified SD-01 and SD-02. Although not required, TSA provided limited notice and opportunity for comment to some pipeline operators and trade associations for SD-01. TSA granted the entities approximately 8 hours to review SD-01 and submit written comments or questions for TSA's consideration. For SD-02, TSA officials provided stakeholders 3 days to review the directive and submit written comments or questions. Trade associations acted as representatives for pipeline operators and provided their comments to TSA. TSA offered limited timeframes for stakeholder feedback because, according to a TSA surface policy official, the security directives required quick issuance to address the immediate cybersecurity vulnerabilities in the pipeline industry.

TSA addressed stakeholder concerns when drafting SD-01 and SD-02. TSA considered the comments submitted by pipeline operators during the drafting process, and we identified changes that appeared to correspond with stakeholder comments. For instance, for SD-01, pipeline operators had concerns with reporting timeframes and overly general terms that TSA did not clearly define, such as "potential cybersecurity incident." In response to the comments submitted, TSA removed "potential" in reference to "cybersecurity incidents" from the final SD-01 to eliminate ambiguity. For SD-02, pipeline operators were concerned that TSA did not consider operational nuances among natural gas utilities, natural gas transmission, and hazardous liquid pipelines and, therefore, the requirements were overly prescriptive. Pipeline operators also commented that TSA's requirement to reset all passwords in

---

[6] 49 U.S.C. § 115(c)(1).

their systems within 30 days was impractical, considering the effort required to update thousands of passwords and that some operators' technology was not compatible with passwords in general. TSA considered stakeholder concerns and changed wording for several requirements and adjusted implementation timelines prior to the release of SD-02 to promote compliance with the directive.

Since their issuance, TSA has made additional changes to the directives' requirements because of stakeholder feedback. On December 1, 2021, SD-01 was replaced by SD-01A, which contained an updated definition of a cybersecurity incident. On May 29, 2022, the directive was again updated to SD-01B, which increased the time to report cybersecurity incidents from 12 to 24 hours. Similarly, SD-02 was replaced by SD-02A on December 10, 2021, and again by SD-02B a week later to include minor updates, such as clarifying implementation timelines for security directive requirements. SD-02 was again updated to SD-02C on July 27, 2022, with significant changes to requirements that are now less prescriptive and provide flexibility in meeting intended security outcomes. For example, SD-02C requires pipeline operators to submit a Cybersecurity Implementation Plan to be approved by TSA that allows for a more flexible, performance-based approach to meet requirements and achieve desired security outcomes. Pipeline operators told us that the changes in SD-02C addressed some of their concerns.

These security directives must be renewed annually to remain in effect. According to TSA officials, the TSA Policy, Plans, and Engagement Office will promulgate formal regulations to replace the security directives, which will make all directive requirements permanent. TSA estimated the notice of proposed rulemaking will be published in September 2023 and regulations will be finalized in 2024.[7]

---

[7] Proposed Rule, Enhancing Surface Cyber Risk Management, 49 C.F.R. § 1570
https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1652-AA74

TSA Did Not Effectively Track Pipeline Operators' Completion of Action Plans

Pipeline operators must comply with TSA's security directives to ensure the safety and security of the pipeline system. When TSA determines an entity is not in compliance with its directives, it uses a progressive enforcement philosophy to promote compliance. Specifically, TSA may attempt to resolve violations through on-the-spot counseling, issuing a warning notice pursuant to 49 CFR § 1503.301, approving action plans under TSA's Action Plan Program, or assessing civil penalties pursuant to 49 CFR § 1503.401.

TSA's Action Plan Program for the security directives allows TSA and pipeline operators to discuss and agree on corrective actions for compliance with security directives without civil penalties. According to TSA officials, before an action plan can be closed, TSA mission support officials must conduct an inspection to confirm compliance.

Based on our review of documentation pipeline operators submitted to TSA, we determined all pipeline operators completed the SD-01 requirements by the required deadline. However, TSA did not effectively track whether all pipeline operators completed the SD-02 requirements by their due dates. SD-02 required pipeline operators to report to TSA when they completed SD-02 requirements. To do so, TSA provided pipeline operators a self-attestation form as an optional tool to report full implementation of SD-02 requirements. Based on our review of TSA action plan information, we determined ██ of the 97 critical pipeline operators did not meet one or more SD-02 requirements, some of which were due in August 2021. In these instances, TSA used action plans and warning notices to bring pipeline operators into compliance with the security directive. TSA approved 259 action plans across ██ pipeline operators and issued 4 warning notices for violations of SD-02 requirements. However, TSA could not easily provide us detailed information, such as which SD-02 requirements remained unresolved.

TSA approved action plans for meeting SD-02 requirements for no more than 60 days, even when a pipeline operator requested more time. TSA can extend action plans an indefinite number of times, and we identified action plans TSA extended numerous times. TSA generally approved all initial action plans as well as applications for extensions if the pipeline operator:

- provided a reasonable explanation for why it could not complete the requirement by the deadline and specified the completion milestones; and
- outlined specific actions and the timeline it would take to complete the requirement.

TSA maintained a spreadsheet tracking the status of action plans, but the information was organized by pipeline operator with requirements grouped together rather than individually tracked. We identified pipeline operators that had multiple action plans for various requirements, which TSA did not list and track separately, making it difficult for TSA to know when each requirement was fulfilled.

During the audit, TSA officials told us that open action plans at the time SD-02C became effective (July 27, 2022) were closed and transferred into a newly required Cybersecurity Implementation Plan (CIP).[8] We did not review SD-02C and the implementation or effectiveness of the CIP.

TSA Did Not Follow Up on Implementation of Mitigation Actions to Address Architecture Design Review and Validated Architecture Design Review Findings

Pipeline operators were required to test the effectiveness of cybersecurity practices by July 26, 2022, through an ADR or validated architecture design review (VADR). An ADR is a third-party evaluation of operational technology design and architecture to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems. CISA conducts VADRs at no charge to the pipeline operator.

CISA's *Operational Resilience Validated Architecture Design Review Standard Operating Procedure,* (October 6, 2020)*,* outlines procedures for the planning, execution, and post-execution phases of VADRs. In the post-execution phase, CISA is to conduct a post-assessment 180 days after completing its VADR to

---

[8] The CIP identifies the SD-02C requirements for pipeline operators that require additional time to complete and establishes a schedule for achieving compliance. According to the directive, the CIP is intended to provide pipeline operators with more flexibility to meet intended security outcomes.

discuss its findings, the pipeline operators' status of any planned or implemented mitigation actions, and the pipeline operators' plans for implementing mitigation actions. SD-02 requires pipeline operators to have a written report detailing the results of the ADR or VADR to be available to TSA upon request.

Of the 97 critical pipeline operators, █ did not complete an ADR by the July 26, 2022 deadline. Because they did not complete the required ADRs, these operators may not have sufficiently identified their cybersecurity vulnerabilities and are, therefore, at greater risk to cybersecurity threats. Furthermore, TSA officials did not request and verify completion of ADR reports from any of the pipeline operators that self-attested to having completed the ADR requirement. As a result, TSA could not ensure pipeline operators mitigated the cybersecurity vulnerabilities identified in these ADRs.

TSA also did not track or follow up on the █ pipeline operators that chose to use a VADR to meet the SD-02 ADR requirement. Further, CISA has not conducted the 180-day post-assessments with █ of the █ pipeline operators. As a result, TSA does not know whether the recommendations presented by CISA have been implemented.

TSA Does Not Have Standard Operating Procedures or a Formal System to Track and Follow Up on the Implementation of the Security Directives

These issues occurred because TSA does not have standard operating procedures or a formal system to track and follow up on the implementation of the security directives. When we asked TSA to provide its procedures related to the pipeline security directives, a TSA official said they did not have standard operating procedures and instead provided an inspection form they used as a guide for documenting whether pipeline operators completed directive requirements. However, the form did not include information such as who was responsible for completing the inspections, when and how the inspections should be performed, or how implementation of the security directive requirements should be tracked and validated.

TSA does not have a formal system to track the implementation of its security directives. As indicated, TSA officials maintain informal records in a spreadsheet, but the information is not easily searchable, does not include

VADR outcomes, and does not state when each requirement was fulfilled or inspected.

Without additional oversight, including a clear process to validate compliance with all security requirements and an improved tracking system, TSA cannot ensure security directives have been fully implemented and that cybersecurity vulnerabilities have been mitigated, which can leave pipeline security at risk of cyber attacks.

Recommendations

Recommendation 1: We recommend the TSA Assistant Administrator for Policy, Plans, and Engagement, in consultation with interagency partners, such as the Department of Transportation, complete rulemaking that will permanently codify critical cybersecurity requirements for pipelines.

Recommendation 2: We recommend the TSA Assistant Administrator for Surface Operations develop standard operating procedures and a formal tracking system to ensure consistent tracking and follow-up of the implementation of security directives and eventual regulations.

Recommendation 3: We recommend the TSA Assistant Administrator for Surface Operations include in TSA's standard operating procedures developed in response to recommendation 2, a requirement to conduct follow-up inspections that ensure pipeline operators have completed mitigation activities to address cybersecurity vulnerabilities.

TSA Comments and OIG Analysis

TSA provided management comments on a draft of this report. TSA concurred with all three recommendations, which we consider open and resolved. In its management response, TSA appreciated that we recognized security directives' positive impacts. However, TSA expressed concerns that we reported delays and difficulties in TSA locating and providing requested information. We included TSA's comments in their entirety in Appendix A. TSA and CISA also provided technical comments, and we revised the report as appropriate. A summary of TSA's response and our analysis follows.

TSA Response to Recommendation 1: Concur. TSA's Policy, Plans, and Engagement Office is working to issue a regulation that will codify critical cybersecurity requirements for pipelines. On November 30, 2022, TSA published the "Enhancing Surface Cyber Risk Management" Advance Notice of Proposed Rulemaking in the Federal Register. TSA sought input on a rulemaking that would establish cybersecurity standards for surface transportation modes determined to have higher risk profiles. The Policy, Plans, and Engagement Office drafted a Notice of Proposed Rulemaking and has a target of the first quarter of fiscal year 2024 for publication of the Notice of Proposed Rulemaking in the Federal Register. Following the close of the public comment period on the Notice of Proposed Rulemaking, TSA will draft a final rule. The target for publication of the final rule is the fourth quarter of fiscal year 2024. Estimated Completion Date (ECD): September 30, 2024.

OIG Analysis of TSA Comments: These actions are responsive to the recommendation, which we consider open and resolved. We will close this recommendation when TSA publishes the final rule.

TSA Response to Recommendation 2: Concur. Surface Operations uses the National Investigations and Enforcement Manual, issued October 2022, and implemented on November 7, 2022, which is the standard operating procedure for how TSA conducts its compliance inspections. Additionally, Surface Operations supplemented the manual using Surface Information Notices and Special Emphasis Inspections, which are formal inspection documents. TSA updates the manual annually.

TSA Surface Operations currently tracks compliance with the Security Directives by using a spreadsheet to record the dates when pipeline operators submitted required documents to TSA. TSA Inspectors also actively inspect companies to verify compliance. TSA tracks inspection scheduling in a separate spreadsheet housed in the Cyber Schedules Teams page on the TSA intranet. TSA's Performance and Results Information System is the authoritative system of record for holding, tracking, and reporting of all TSA inspections. TSA also supplements the system with other internally-developed tools. Based on the procedures and tracking systems in place, TSA requested that we consider this recommendation resolved and closed, as implemented.

OIG Analysis of TSA Comments: TSA's actions are partially responsive to the recommendation, which we consider open and resolved. The manual, which TSA provided us after our draft report was issued, has robust instructions on conducting physical security compliance inspections. However, the document lacks procedures for conducting cybersecurity-related inspections. Further, as we noted in the audit report, TSA could improve its system of using multiple spreadsheets to track inspection outcomes, follow-ups, and implementation of security directive requirements. We will close this recommendation when TSA provides an updated version of the manual or other operating procedures that include procedures for conducting cybersecurity-related inspections and documentation demonstrating how TSA uses the system to track the implementation of security directive requirements.

TSA Response to Recommendation 3: Concur. On July 21, 2022, TSA Policy, Plans, and Engagement Office issued SD Pipeline 2021-02C: "Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing" with an effective date of July 27, 2022. The new SD transitioned to a more flexible, performance-based approach and required all pipeline operators to create a CIP within 90 days and submit the plan to TSA for approval. The CIP will set the security measures and requirements that TSA will use to inspect for compliance.

TSA received CIPs from all SD-covered operators and approved those CIPs as of February 14, 2023. In addition to the CIP, TSA requires operators to submit a Cybersecurity Assessment Plan (CAP) to TSA no later than 60 days after the CIP approval. All operators submitted their required CAPs to TSA as of April 14, 2023. Further, the Policy, Plans, and Engagement Office updated the SD Pipeline-2021-02 series in July 2023, providing timelines for TSA review and approval of operators' CAPs annually. TSA requested that we consider this recommendation resolved and closed, as implemented.

OIG Analysis of TSA Comments: These actions are partially responsive to the recommendation, which we consider open and resolved. We will close this recommendation when TSA provides an updated manual or other operating procedures that includes detailed procedures TSA employees will use to follow up with pipeline operators to ensure completion of the mitigation activities outlined in their CIPs and CAPs to address vulnerabilities.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978.*

We audited TSA's pipeline security directives issued in 2021. The objective of our audit was to determine whether TSA's 2021 security directives addressed cyber threats and stakeholder concerns and strengthened pipeline security.

To accomplish our objective, we reviewed Federal laws and regulations, as well as applicable DHS, TSA, and CISA policies and guidance. We reviewed TSA's and CISA's internal controls to determine whether they were properly designed, implemented, and operating effectively. We reviewed U.S. Government Accountability Office reports related to our audit objective to gain an understanding of their findings. Additionally, we interviewed TSA and CISA officials from headquarters and field locations. We reviewed security directive documents, pre-decisional and final versions of SD 2021-01 and SD 2021-02 and determined the requirements pipeline operators were to fulfill. We reviewed pipeline operators' comments on the drafts of SD-01 and SD-02 and gained an understanding of stakeholder concerns and how they were addressed by TSA. We reviewed TSA's action plan information, warning notices, inspection reports, and CISA's VADR reports to determine the extent of pipeline operators' implementation of SD-02.

We conducted on-site and phone interviews with four pipeline operators and determined how the directives affected their operations. We also reviewed and analyzed TSA and CISA data related to SD-01 and SD-02, including critical pipeline ranking information, ADR and VADR information, action plan information, and warning notices, and determined the information was sufficiently reliable to support the findings and conclusions made in our audit report.

We conducted this performance audit between April 2022 and June 2023 pursuant to the *Inspector General Act of 1978,* 5 U.S.C. § 401–424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and

conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

The Office of Audits major contributors to this report are Yesi Starinsky, Director; Ruth Blevins, Director; Andrew Smith, Audit Manager; Douglas Campbell, Audit Manager; Daniel Malone, Auditor-in-Charge; Keith Lutgen, Auditor; Tom Hamlin, Communications Analyst; and Stuart Josephs, Independent Report Referencer.

DHS OIG's Access to DHS Information

During this audit, TSA did not provide us with requested information concerning TSA's tracking of pipeline operators' compliance with SD-02 requirements, citing difficulties in locating the information and lack of completeness. Ultimately, we determined this was a reportable finding as reflected in recommendation 2 in the report.
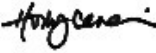
Appendix A
TSA Comments to the Draft Report

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

August 23, 2023

MEMORANDUM FOR: Joseph V. Cuffari, PhD
                               Inspector General

FROM: Holly Canevari
                             Deputy Administrator (Acting)
                             Transportation Security Administration

SUBJECT: Management Response to Draft Report: "Better TSA
                             Tracking and Follow-up for the 2021 Security Directives
                             Implementation Should Strengthen Pipeline Cybersecurity"
                             (Project No. 22-017-AUD-CISA, TSA)

Thank you for the opportunity to comment on this draft report. The Transportation Security Administration (TSA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

TSA leadership is pleased to note OIG's recognition of the two Security Directives issued in 2021—Security Directive Pipeline–2021–01, "Enhancing Pipeline Cybersecurity"[1] and Security Directive Pipeline–2021–02 "Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing"[2]— and the positive impacts they are having on the Nation's pipeline infrastructure to defend against cyber threats. OIG also acknowledged TSA's collaboration with stakeholders when drafting the directives, which was vital to ensure a complete picture of perspectives and input were incorporated.

TSA values its partnership with DHS Components, the interagency, industry partners, and others to address ongoing and rising threats to pipeline infrastructure. TSA remains committed to strengthening cybersecurity throughout all modes of transportation, including pipeline.

However, TSA leadership is concerned about the assertions OIG made in the draft report section entitled "DHS OIG's Access to DHS Information." OIG alleged that TSA had

---

[1] Security Directive Pipeline-2021-01 was originally issued on May 26, 2021, and most recently reissued as Pipeline-2021-01B on May 27, 2022
[2] Security Directive Pipeline 2021-02 was originally issued on July 19, 2021, and most recently reissued as Pipeline-2021-02C on July 21, 2022. This Security directive continues, under a new performance-based regulatory model, mandatory cybersecurity measures first implemented by TSA in July 2021

difficulties in locating and providing complete information to the audit team on tracking pipeline operators' compliance with "Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing" (2021-02) requirements. TSA has tracking mechanisms in place as discussed further in response to Recommendation 2 below. Further, TSA uses multiple platforms to track compliance with inspection requirements.

The draft report contained three recommendations with which TSA concurs. Enclosed, find our detailed response to each recommendation. TSA previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Enclosure

Management Response to Recommendations
Contained in OIG 22-017-AUD-CISA, TSA

OIG recommended that the TSA Assistant Administrator for Policy, Plans and Engagement:

Recommendation 1: In consultation with interagency partners, such as the Department of Transportation, complete rulemaking that will permanently codify critical cybersecurity requirements for pipelines.

Response: Concur. TSA's Policy, Plans, and Engagement (PPE) office is working to issue a regulation that will codify critical cybersecurity requirements for pipelines. On November 30, 2022, TSA published the "Enhancing Surface Cyber Risk Management"[3] Advance Notice of Proposed Rulemaking (ANPRM) in the *Federal Register*. TSA sought input on a rulemaking that would establish cybersecurity standards for surface transportation modes determined to have higher risk profiles. The comment period for the advanced notice closed on January 17, 2023.

TSA PPE has reviewed and considered those comments in the draft regulation. TSA PPE drafted an NPRM and has a target of quarter 1 of fiscal year 2024 for publication of the NPRM in the *Federal Register*. Following the close of the public comment period on the NPRM, TSA will draft a final rule. The target for publication of the final rule is quarter 4 of fiscal year 2024. Estimated Completion Date (ECD): September 30, 2024

OIG recommended that the TSA Assistant Administrator for Surface Operations:

Recommendation 2: Develop standard operating procedures and a formal tracking system to ensure consistent tracking and follow-up of the implementation of security directives and eventual regulations.

Response: Concur. Surface Operations uses the National Investigations and Enforcement Manual ((NIEM), issued October 2022, and implemented on November 7, 2022), which is the standard operating procedure on how TSA conducts its compliance inspections. Additionally, Surface Operations has supplemented the NIEM by creating formal inspection documents in the form of Surface Information Notices (SIN) and Special Emphasis Inspections (SEI). The NIEM is updated annually.

TSA Surface Operations currently tracks compliance with the Security Directives by using a spreadsheet to record the dates when required documents were submitted to TSA.

---

3 https://www.federalregister.gov/documents/2022/11/30/2022-25941/enhancing-surface-cyber-risk-management

TSA Inspectors are also actively inspecting companies to verify compliance. Inspection scheduling is tracked in another spreadsheet housed in the Cyber Schedules Teams page on the TSA intranet. TSA's Performance and Results Information System (PARIS) is the authoritative system of record for holding, tracking, and reporting of all TSA inspections. PARIS is also supplemented by other internally developed tools.

Based on the procedures and tracking systems in place, TSA requests OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Include in TSA's standard operating procedures developed in response to recommendation 2, a requirement to conduct follow-up inspections that ensure pipeline operators have completed mitigation activities to address cybersecurity vulnerabilities.

Response: Concur. On July 21, 2022, TSA PPE issued SD Pipeline 2021-02C: "Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing"[4] with an effective date of July 27, 2022, which canceled and superseded Security Directive Pipeline–2021–02B: "Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing" (SD-02B). The new SD transitioned to a more flexible, performance-based approach and required all pipeline operators to create a Cybersecurity Implementation Plan (CIP) within 90 days and submit the plan to TSA for approval. The CIPs will set the security measures and requirements against which TSA will inspect for compliance.

TSA received CIPs from all SD-covered operators and approved those CIPs as of February 14, 2023.

In addition to the CIP, operators are required to submit a Cybersecurity Assessment Plan (CAP) to TSA no later than 60 days after the CIP approval. All operators submitted their required CAPs to TSA as of April 14, 2023. Further, PPE updated the SD Pipeline-2021-02 series in July 2023, providing timelines for TSA review and approval of operators' CAPs annually.

TSA requests that OIG consider this recommendation resolved and closed, as implemented.

---

[4] https://www.tsa.gov/sites/default/files/tsa_sd_pipeline-2021-02-july-21_2022.pdf

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
TSA Administrator
CISA Director
TSA Liaison
CISA Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees
Sam Graves, Ranking Member Committee on Transportation and Infrastructure
Rick Crawford, Ranking Member Subcommittee on Rail, Pipelines, and Hazardous Materials
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

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click
on the red "Hotline" box. If you cannot access our website, call our hotline at
(800) 323-8603, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305