



This document is scheduled to be published in the Federal Register on 2026-04-23 and available online at <https://www.federalregister.gov/d/2026-0785Z>, and on <https://govinfo.gov>

BILLING CODE 9110-05-P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request Approval from OMB of One New Public Collection of Information: Insider Threat Incident Reporting Tool

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on a new Information Collection Request (ICR) abstracted below that we will submit to the Office of Management and Budget (OMB) for approval in compliance with the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. The collection involves the submission of details by the public, concerning potential insider threats, as well as any pertinent information regarding the person(s) involved in the reported event.

DATES: Send your comments by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Comments may be e-mailed to TSAPRA@tsa.dhs.gov or delivered to the TSA PRA Officer, Information Technology, TSA-11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6011.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh at the above address, or by telephone (571) 227-2062.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a

collection of information unless it displays a valid OMB control number. The ICR documentation will be available at <https://www.reginfo.gov> upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to--

- (1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
- (2) Evaluate the accuracy of the agency's estimate of the burden;
- (3) Enhance the quality, utility, and clarity of the information to be collected; and
- (4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

Under the Aviation and Transportation Security Act, TSA is responsible for security in all modes of transportation, including screening operations for passenger air transportation and for carrying out such other duties it considers appropriate relating to transportation security.¹ Under DHS Instruction 262-05-002, "*Information Sharing and Safeguarding: Insider Threat Program*," issued on October 1, 2019, DHS established requirements, standards, and assigned responsibilities for DHS agencies to implement an insider threat detection and prevention program. This document also defines "Insider Threat" and "Insider." An "insider" is any person who has or who had authorized access to any DHS facility, information, equipment, network, or system. An "Insider Threat" is defined as the

¹ See sec. 101(a) of the Aviation and Transportation Security Act, Pub. L. 107-71 (115 Stat. 597-598, Nov. 19, 2001), as codified at 49 U.S.C. § 114(d) and (f). See also Memorandum, *Expanding the Scope of the Department of Homeland Security Insider Threat Program* (submitted Dec. 7, 2016, approved Jan. 3, 2017); Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012); Executive Order 13587, *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 76 FR 63811 (October 7, 2011).

threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems.

TSA created the Insider Threat Program in compliance with the DHS Instruction's requirements for DHS components. The program's purpose is to detect, deter, and mitigate threats that an individual with authorized access to sensitive areas and/or information, wittingly or unwittingly misuse or allow others to misuse this access to exploit vulnerabilities in an effort to compromise security, facilitate criminal activity, terrorism, or other illicit actions that inflict harm to people, organizations, the transportation system, or national security, including transportation sector personnel, operations, information, systems and critical infrastructure. The program operates as a partnership among TSA, aviation, mass transit, and maritime sectors, as well as with state and local law enforcement.

To ensure consistency with the directive, TSA created the Insider Threat Reporting Tool, which collects information on potential insider threats. TSA is requesting OMB's approval of the Insider Threat Incident Reporting Tool as a Common Form to permit Federal agency users beyond the agency that created the form (e.g., DHS or U.S. Office of Personnel Management) to streamline the information collection process in coordination with OMB.

Purpose and Description of Data Collection

The Insider Threat Incident Reporting Tool is an online application where the public can submit inquiries regarding potential insider threats by providing personal information and other specific data regarding the person or situation deemed to be an insider threat. TSA uses the information collected to review the potential insider threats and to determine if further evaluation and follow-up is necessary. The collection may include individual personal information and/or appearance, and the details surrounding

the situation alleged to be the potential insider threat. TSA requires submitters to attest that all information submitted is true.

The likely respondents to this proposed information collection are any person who has or who had authorized access to any DHS facility, information, equipment, network, or system, including individuals detailed or assigned to DHS. TSA estimates that an average of approximately 312 respondents will be completing the Insider Threat Incident Reporting Tool annually. TSA estimates that it takes approximately 10 minutes (0.16667 hours) to complete and submit the report, resulting in the annual burden of 52 hours.

Use of Results

TSA Insider Threat Reporting Tool will use the reported information to detect, prevent and mitigate threats. In compliance with the Government Paperwork Elimination Act, the collection uses an online web tool, available at <https://www.tsa.gov/travel/insider-threat>. All submissions are sent through a secure TSA internal network drive accessible only by authorized personnel. TSA will protect the information in accordance with DHS Directive 262-05-002.

Dated: April 20, 2026.

Christina A. Walsh,

Paperwork Reduction Act Officer,

Information Technology,

Transportation Security Administration.