This document is scheduled to be published in the
Federal Register on 07/29/2025 and available online at
https://federalregister.gov/d/2025-14231, and on **https://govinfo.gov**

9111-LF

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2023-0038]

Agency Information Collection Activities**:** Office for Bombing Prevention – Technical Analytics

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 30- Day Notice and request for comments; Information Collection Request, 1670-0028.

SUMMARY: The OFFICE FOR BOMBING PREVENTION (OBP) within Cybersecurity and Infrastructure Security Agency (CISA) will submit the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. CISA previously published this information collection request (ICR) in the ***Federal Register*** on January 10th, 2025, for a 60-day public comment period. ZERO comments were received by CISA. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This process is conducted in accordance with 5 CFR 1320.10. This is a reinstatement of an existing collection (1670-0028) with changes to the information collection.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain . Find this particular information collection by selecting "Currently under 30-day Review - Open for Public Comments" or by using the search function.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information 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 of the proposed collection of information, including the validity of the methodology and assumptions used;
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 through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

FOR FURTHER INFORMATION CONTACT: Dennis Molloy, 202-604-3512, dennis.molloy@mail.cisa.dhs.gov.

SUPPLEMENTARY INFORMATION:

Technical Resource for Incident Prevention (TRIPwire)

TRIPwire (Technical Resource for Incident Prevention) is the Department of Homeland Security's online, collaborative information-sharing network for bomb technicians, first responders, military personnel, government officials, intelligence analysts, and select private sector security professionals to increase awareness of evolving improvised explosive device (IED) tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information. Developed and maintained by OBP, the TRIPwire system combines expert analysis and reports with relevant documents, images, and videos gathered from publicly available sources to help users anticipate, identify, and prevent IED incidents.

Users from federal, state, local, and tribal government entities, as well as business and/or other for-profit industries, can register for TRIPwire access. The TRIPwire portal contains sensitive information related to the criminal use of explosives by threat actors, including violent, malicious organizations, which requires a limited, controlled means of dissemination—such as designations of "For Official Use Only," "Law Enforcement Sensitive," or "Controlled Unclassified Information." Therefore, CISA must collect user information in order to verify an individual's eligibility to access the TRIPwire system.

In addition to new user registrations, CISA will also seek feedback from TRIPwire users via a questionnaire and will request that TRIPwire users revalidate their access status on an annual basis. All information collected/provided pursuant to this ICR will be done so on a strictly voluntary basis.

This collection of information is consistent with CISA's statutory authorities to provide assistance to federal and non-federal entities to enhance the security and resiliency of critical infrastructure, including the authority provided by 6 U.S.C. § 652(c)(5), (11) and 6 U.S.C. § 652(e)(1)(C). The previous Federal Register notice incorrectly stated the Total Burden Cost stated as $13,736 when it should have been $16,333. The Total annualized Government Cost stated as $7,447 was also incorrect as it should have been $8,209. The correct costs are also reflected in the Analysis section below.

ANALYSIS:

Agency: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

Title: Office For Bombing Prevention Technical Analytics.

OMB Number: 1670-0028.

Frequency: Quarterly to Annually.

Affected Public: Federal, state, local, and tribal government entities, and business or other for-profit.

Number of Respondents: 4,333.

Estimated Time Per Respondent: 5 minutes.

Total Burden Hours: 422 Hours.

Total Annual Burden Cost: $16,333

Total Annual Government Burden Cost: $8,209.

Robert J. Costello,
Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2025-14231 Filed: 7/28/2025 8:45 am; Publication Date: 7/29/2025]