

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 submission of responses.

**Maile Rasco-Arthur,**

*Deputy Director for Information Management, Office of the Chief Administrative Officer, Mission Support, Federal Emergency Management Agency, Department of Homeland Security.*

[FR Doc. 2023-18586 Filed 8-28-23; 8:45 am]

BILLING CODE 9111-78-P

**DEPARTMENT OF HOMELAND SECURITY**

[Docket No. CISA-2023-0021]

**Agency Information Collection Activities: Gratuitous Services Agreement, Volunteer Release and Hold Harmless, and OBP Interest Sign-Up Sheet**

**AGENCY:** Cybersecurity and Infrastructure Security Agency, DHS.

**ACTION:** 60-Day notice and request for comments; Extension without changes, 1670-0031.

**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. The following forms of information collection to include the Voluntary Participation Release of Liability Agreement, the Gratuitous Services Agreement and the OBP interest sign-up sheet are renewals of an existing collection and no changes were made to the collection instruments.

**DATES:** Comments are encouraged and will be accepted until October 30, 2023.

**ADDRESSES:** You may submit comments, identified by docket number Docket # CISA-2023-0021, at:

○ *Federal eRulemaking Portal:* <https://www.regulations.gov>. Please follow the instructions for submitting comments.

*Instructions:* All submissions received must include the agency name and docket number Docket # CISA-2023-0021. All comments received will be posted without change to <https://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket to read background documents or

comments received, go to <https://www.regulations.gov>.

**SUPPLEMENTARY INFORMATION:** Under the Homeland Security Presidential Directive-19: Combating Terrorist Use of Explosives in the United States, the Department of Homeland Security (DHS) was mandated to educate private sector security providers about IED threats, including tactics, techniques, and procedures relevant to their usage, so they are knowledgeable about terrorist use of explosives and contribute to a layered security approach.

The President's Policy Directive-17: Countering Improvised Explosive Devices (PPD-17) reaffirms the 2007 Strategy for Combating Terrorist Use of Explosives in the United States. It provides guidance to update and gives momentum to our ability to counter threats involving improvised explosive devices (IEDs). DHS was mandated to deliver standardized IED awareness and familiarization training for federal, state and local responders and public safety personnel.

Over the past 10 years, incidents involving IEDs has increased worldwide. This highlights the existing threat of IED attacks by terrorists, transnational criminal organizations, and individuals domestically that have radical political, environmental, or international viewpoints. IEDs have been used in the theater of war, mass transit systems overseas (London, Spain), in global aviation plots (December 2009), assignation attempts against political leaders, and other attempts here within the United States (Portland, Times Square, Boston Marathon 2013). They have also been used to threaten our ability in the secure movement of goods in accordance with the National Strategy for Global Supply Chain Security (print cartridge).

The Office for Bombing Prevention (OBP) must collect this information to effectively deliver training without concern that an individual who acts as a volunteer role player in support of official OBP training sustains an injury or death during the performance of his or her supporting role. Additionally, OBP must collect conference attendee information to properly identify key stakeholder segments and to ensure ongoing engagement and dissemination of OBP products to those who desire them.

The purpose of the Volunteer Participant Release of Liability Agreement is to collect necessary information in case an individual who acts as a volunteer role player in support of official OBP training sustains

an injury or death during the performance of his or her supporting role. If legal action is taken, this information can serve as a "hold harmless" statement/agreement by the Government. In the unlikely event that an injury or death is sustained in the performance of support for training, this information will be used by CISA/IP/PSCD/OBP to protect against legal action by the volunteer or their family. If legal action is taken, this information can serve as a "hold harmless" statement/agreement by the Government.

The purpose of the Gratuitous Services Agreement is to establish that no monies, favors or other compensation will be given or received by either party involved. The information from the Gratuitous Services Agreement will be used by CISA/IP/PSCD/OBP in the event that questions arise regarding remuneration or payment for volunteer participation in training events.

The purpose of the OBP interest sign-up sheet is to collect basic contact information, on a voluntary basis, of those who attend the OBP conference booth and desire further engagement or additional products from OBP. The information is used by OBP to follow-up with the individuals who provide their contact information.

Additional considerations for these forms:

- The two training forms are best delivered as hard copies to volunteer participants that attend the courses to ensure the right audiences are targeted in an environment where last-minute changes to the participant list are common. However, it is feasible that these forms will transition to a Learning Management System (LMS) enabling participants to complete online.

- The OBP interest sheet is a hard copy form laid on OBP's booth table for attendees to provide their contact information. There has been some consideration to shifting this to an electronic format, but current booth technology does not fully support this transition.

- These forms do not negatively affect small businesses.

- Failure to collect this information could result in questions of liability and/or remuneration for volunteers in IP/OBP and reluctance to seek volunteer involvement as a result. This would negatively affect the overall quality of the program in delivering these trainings to private sector security providers, federal, state and local responders, and public safety personnel.

- Failure to collect contact information from those who visit the

OBP booth would greatly limit OBP's ability to stay engaged with or grow its stakeholder base or provide the most relevant products/services to those stakeholders.

- This collection does not include a pledge of confidentiality that is not supported by established authority in statute or regulation. This collection of information is covered by PIA DHS/ALL/PIA-006 DHS General Contact List.

- This is a renewal of an existing collection. No changes were made to the collection instruments.

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.

#### Analysis

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

*Title:* Gratuitous Services Agreement, Volunteer Release and Hold Harmless, and OBP Interest Sign-up Sheet.

*OMB Number:* 1670-0031.

*Frequency:* Annually.

*Affected Public:* STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS AND PRIVATE SECTOR INDIVIDUALS.

*Number of Respondents:* 950.

*Estimated Time per Respondent:* 15 MIN.

*Total Burden Hours:* 160.

*Total Annualized Respondent Cost:* \$6,812.

*Total Annualized Respondent Out-of-Pocket Cost:* \$0.

*Total Annualized Government Cost:* \$21,204.

**Robert J. Costello,**

*Chief Information Officer, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.*

[FR Doc. 2023-18556 Filed 8-28-23; 8:45 am]

**BILLING CODE 9110-9P-P**

## DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2023-0010]

### Agency Information Collection Activities: Sector Outreach and Programs Online Meeting Registration Tool

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

**ACTION:** 30-Day notice and request for comments; revision; 1670-0019.

**SUMMARY:** The Infrastructure Security Division (ISD) 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. The submission proposes to renew the information collection for an additional three years and update the burden estimates associated with collecting information for the purposes of registration for meetings and events. CISA previously published this information collection request (ICR) in the **Federal Register** on April 5, 2023 for a 60-day public comment period. No comments were received by CISA. The purpose of this notice is to allow additional 30-days for public comments.

**DATES:** The comment period for the information collection request published on April, 05, 2023 at 88 FR 20176. Comments are encouraged and will be accepted until September 28, 2023.

**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](http://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.

**FOR FURTHER INFORMATION CONTACT:** Annie Hunziker Boyer, 703-603-5000, [CISARegulations@cisa.dhs.gov](mailto:CISARegulations@cisa.dhs.gov).

**SUPPLEMENTARY INFORMATION:** The Critical Infrastructure Protection Act of

2001, 42 U.S.C. 5195c, states that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States; and that actions necessary to achieve the policy stated be carried out in a public-private partnership involving corporate and non-governmental organizations. On behalf of the DHS, the Cybersecurity and Infrastructure Security Agency's Infrastructure Security Division (CISA ISD) manages the Department's program to protect the Nation's 16 critical infrastructure sectors by implementing the National Infrastructure Protection Plan (NIPP) 2013, Partnering for Critical Infrastructure Security and Resilience. Pursuant to Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience (February 2013), each sector is assigned a Sector-Specific Agency (SSA) to oversee Federal interaction with the array of sector security partners, both public and private. An SSA is responsible for leading a unified public-private sector effort to develop, coordinate, and implement a comprehensive physical, human, and cyber security strategy for its assigned sector. There are six critical infrastructure sectors assigned to CISA ISD, including the Chemical sector. In addition to fulfilling the regulatory obligations set forth by Congress, the CISA Office of Chemical Security coordinates with the builds sustainable partnerships with its public and private sector stakeholders to enable more effective coordination, information sharing, and program development and implementation. These partnerships are sustained through the NIPP Sector Partnership Model.<sup>1</sup>

Information sharing is a key component of the NIPP Partnership Model, and DHS sponsored conferences are one mechanism for information sharing. To facilitate conference planning and organization. This voluntary information collection tool for online event registration is maintained and leveraged by the Office of Chemical Security within CISA ISD. The information collected with this tool is used to register public and private sector stakeholders for meetings hosted by the Office of Chemical Security, principally the annual Chemical Security Summit. This tool is also used for private sector stakeholders to register their interest in being contacted by

<sup>1</sup> NIPP 2013 Partnering for Critical Infrastructure Security and Resilience, pp 10-12.