requiring them all, a related programming update will enable trade participants the ability to modify or change a previous enrollment, including updating or adding additional GBI numbers, which may include a variety of global identifier types (LEI, GLN, DUNS). This programming change would provide more flexibility and utility to GBI participants by enabling GBI numbers to be provided voluntarily when they are known and encourages participants to obtain other GBI numbers as well as keep supply chain information current because they can easily add, delete, and modify GBI numbers associated to an enrollment.

3. The GBI Test is also expanding the available GBI supply chain entity party types from the original six optional parties (Manufacturer, Shipper, Seller, Exporter, Distributor, Packager), to include two new parties: ''Intermediary'' and ''Source,'' along with optional free text fields for all the parties that will allow filers to voluntarily input additional descriptions and information about the specific party type or the underlying entity. These party types and the free text fields would be made available in the GBI Enrollment database as well as in ACE Cargo Release. Collectively, the updates aim to enhance upstream supply chain traceability and visibility while addressing the increasing complexity of global trade supply chains. All participation and data is voluntary.

4. As a demonstration of CBP's intent to expand the choices of identifiers available to filers over the duration of the Test, CBP is also working to add new voluntary GBI identifiers, beginning with the Altana ID (ALTA) maintained by Altana Technologies USG Inc. (Altana), as announced on August 8, 2025 in the **Federal Register** (*See,* 90 FR 38479). At no cost to the government to access the underlying entity and product specific supply chain data associated with an ALTA, this identifier offers comprehensive insights across a product's supply chain, thereby enhancing traceability for CBP which may translate to facilitation benefits and reduced industry costs. CBP has initiated programming requests to create an ALTA GBI field in ACE and to increase the current character limit in ACE allowed for GBI identifiers. The addition of the ALTA identifier alongside the current GBI identifiers will widen participants' choices and allow CBP to continue to evaluate the breadth and veracity of entity and supply chain information embedded within different types of identifier solutions already being leveraged by trade industry traceability stewards. It will also contribute to CBP's ongoing exploration of how traced supply chain information may be ingested and operationalized for risk management and facilitation purposes. CBP proposes adding more participants as the test continues, and with approval from OMB, will add these to the collection through a non-substantive change to the collection.

CBP encourages the trade to comment specifically on whether there are other comparable identifiers that the trade already has, or that it would be advantageous for CBP to include.

Section 484 of the Tariff Act of 1930, as amended (19 U.S. Code 1484) and Part 141, Code of Federal Regulations, Title 19 (19 CFR part 141), pertain to the entry of merchandise and authorize CBP to require information that is necessary for CBP to determine whether merchandise may be released from CBP custody. Provisions of the U.S. Code and CBP regulations, in various parts and related to various types of merchandise, specify information that is required for entry. For reference, Part 163, Code of Federal Regulations, Title 19 (19 CFR part 163 Appendix A) refers to a wide variety of regulatory provisions for certain information that may be required by CBP.

Type of Information Collection: Global Business Identifier (GBI).

Estimated Number of Respondents: 100.

Estimated Number of Annual Responses per Respondent: 1.

Estimated Number of Total Annual Responses: 100.

Estimated Time per Response: 10 minutes.

Estimated Total Annual Burden Hours: 17.

Dated: August 26, 2025.

Seth D. Renkema,

Branch Chief, Economic Impact Analysis Branch, U.S. Customs and Border Protection.

[FR Doc. 2025–16547 Filed 8–27–25; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0012]

Agency Information Collection Activities: Infrastructure Visualization Platform (IVP) Pre-Collection Questionnaire

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

ACTION: 30-Day notice and request for comments; new information collection request, 1670–NEW.

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. CISA previously published this information collection request (ICR) in the **Federal Register** on May 21, 2024 for a 60-day public comment period. 0 comments were received by CISA. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until September 29, 2025.

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: If additional information is required contact: Jonathan Moaikel; 202–251–5276; *jonathan.moaikel@mail.cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: CISA's ISD supports the homeland security mission of critical infrastructure security. As part of this mission, CISA Protective Security Advisors (PSAs)

conduct various critical infrastructure security assessments for various stakeholders including facility owners and operators; federal, state, and local law enforcement officials; emergency response personnel; and others.

One type of assessment PSAs can perform is an Infrastructure Visualization Platform (IVP). IVPs integrate high-resolution, interactive visual data as well as additional assessment information. For a PSA to conduct an assessment, each stakeholder must complete an IVP Pre-Collection Questionnaire. The questionnaire requests information such as the purpose of the IVP assessment being requested, the security point of contact the team will be meeting with when they arrive at the facility, who will be escorting the team as they tour the facility, special considerations the collection team need to plan for prior to arriving at the facility, and priority areas know as Areas of Emphasis that the team should be focused on while conducting the IVP assessment collection. When the form is completed and submitted, the IVP team can better plan for the assessment by reviewing locations designated as Areas of Emphasis (AOEs) to ensure those areas receive an assessment, to know who appropriate points of contact are (stakeholder requesting and escort who will be with the team during the collect), and to address special considerations prior to showing up for the collect.

Analysis

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

Title of Collection: Infrastructure Visualization Platform (IVP) Pre-Collection Questionnaire.

OMB Control Number: 1670–NEW.

Frequency: Annually.

Affected Public: State, local, Tribal, Territorial Governments and Private Sector Individuals.

Number of Respondents: 120.

Estimated Time per Respondent: 30 minutes.

Total Burden Hours: 60 hours.

Annualized Respondent Cost: $2,527.00.

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

Total Annualized Government Cost: $2,576.00.

Robert J. Costello,

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

[FR Doc. 2025–16489 Filed 8–27–25; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; SAFECOM Membership Questionnaire

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

ACTION: 30-Day notice of information collection; request for comment; reinstatement, with change, of a previously approved collection for which approval has expired.

SUMMARY: The Emergency Communications Division (ECD) within Cybersecurity and Infrastructure Security Agency (CISA) submits the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance. CISA previously published this information collection request (ICR) in the **Federal Register** on May 26, 2025, for a 60-day public comment period. Zero comments were received by CISA. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until September 29, 2025.

Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: You may submit comments, identified by docket number CISA–2025–0005, by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.
- *Instructions:* All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided.

Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an email comment, your email address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public notwithstanding the inclusion of the routine notice.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Ralph Barnett III, at (703) 705–6130, or email at *SAFECOMGovernance@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: On November 16, 2018, Congress passed Public Law 115–278, to amend the Homeland Security Act of 2002 (6 U.S.C. 101 *et seq.*), enacted and authorized the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS). CISA enhances public safety interoperable communications at all levels of government to help partners across the country develop their emergency communications capabilities. Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of a natural disaster, act of terrorism, or other man-made disaster. 6 U.S.C. 571(c)(2) mandates DHS through CISA to administer and manage the Department's authorities and responsibilities relating to the SAFECOM program, a state, local, tribal, and territorial stakeholder-driven public safety communications program. In an effort to resolve major communications issues identified during the September 11, 2001 terrorist attacks, SAFECOM was created as a Presidential E Government Initiative to improve interoperability, allowing emergency responders to communicate more effectively before, during, and after emergencies and disasters.

Through collaboration with emergency responders and elected officials across all levels of government, SAFECOM works to improve emergency response providers' inter-jurisdictional and interdisciplinary emergency communications interoperability across local, regional, tribal, State, territorial, international borders, and with Federal government entities. SAFECOM works with existing Federal communications programs and key emergency response stakeholders to address the need to develop better technologies and processes for the coordination of existing communications systems and future networks.

The SAFECOM Membership Questionnaire is an internal SAFECOM document disseminated only to active