Submitting Comments

We encourage you to submit comments through the Federal eRulemaking Portal at *https://www.regulations.gov.* If your material cannot be submitted using *https://www.regulations.gov,* contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions. Documents mentioned in this notice, and all public comments, are in our online docket at *https://www.regulations.gov* and can be viewed by following that website's instructions. If you go to the online docket and sign up for email alerts, you will be notified when comments are posted.

We accept anonymous comments. Comments we post to *https://www.regulations.gov* will include any personal information you have provided. For more about privacy and submissions to the Coast Guard in response to this document, see DHS's eRulemaking System of Records notice (85 FR 14226, March 11, 2020). For more about privacy and submissions to OIRA in response to this document, see the *https://www.reginfo.gov,* comment-submission web page. OIRA posts its decisions on ICRs online at *https://www.reginfo.gov/public/do/PRAMain* after the comment period for each ICR. An OMB Notice of Action on each ICR will become available via a hyperlink in the OMB Control Number: 1625–0122.

Previous Request for Comments

This request provides a 30-day comment period required by OIRA. The Coast Guard published the 60-day notice (90 FR 40610, August 20, 2025) required by 44 U.S.C. 3506(c)(2). That notice elicited no comments. Accordingly, no changes have been made to the Collection.

Information Collection Request

Title: Cargo Securing Manuals.

OMB Control Number: 1625–0122.

Summary: The information is used by the Coast Guard to review/approve new or updated cargo securing manuals (CSM).

Need: 46 U.S.C. 2103 and 3306 authorizes the Coast Guard to establish these regulations. Title 33 CFR 97 prescribes the CSM regulations.

Forms: None.

Respondents: Owners, operators, and masters of certain cargo vessels.

Frequency: On occasion.

Hour Burden Estimate: The estimated burden has decreased from 280 hours to 260 hours a year, due to a decrease in the estimated annual number of CSM submissions.

Authority: The Paperwork Reduction Act of 1995; 44 U.S.C. chapter 35, as amended.

Dated: October 31, 2025.

Bradley E. White,

(Acting) Chief, Office of Privacy Management, U.S. Coast Guard.

[FR Doc. 2025–21468 Filed 11–26–25; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2025–0002]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Visitor Request Form

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

ACTION: 30-Day notice of Information Collection; request for comment; This a renewal of existing 11000–39 Visitor Request Form, 1670–0036 that was previously approved on August 05, 2022, with an expiration date of November 30, 2025.

SUMMARY: The Office of the Chief Security Officer (OCSO) 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 August 20, 2025, for a 60-day public comment period. No 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 December 29, 2025. Submissions received after the deadline for receiving comments may not be considered.

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: Michael A. Washington, Jr., 703–235–1925, *Michael.Washington@mail.cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: Public Law 107–296 The Homeland Security Act of 2002, Title II, recognizes the Department of Homeland Security's role in integrating relevant critical infrastructure and cybersecurity information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities while maintaining positive control of sensitive information regarding the national infrastructure. In support of this mission, CISA Office of the Chief Security Officer (OCSO) must maintain a robust visitor screening capability. CISA OCSO will collect, using an electronic form, information about each potential visitor to CISA facilities and the nature of each visit. CISA OCSO will use collected information to make a risk-based decision to allow visitor access to CISA facilities. This is an extension of an existing information collection.

Analysis

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

Title: Cybersecurity and Infrastructure Security Agency (CISA) Visitor Request Form.

OMB Number: 1670–0036.

Frequency: Annually.

Affected Public: Private and Public Sector.

Number of Respondents: 20,000.

Estimated Time Per Respondent: 10 minutes.

Total Burden Hours: 3,333 hours.

Total Annual Burden Cost: $158,010.66.

Total Government Burden Cost: $366,514.16.

Robert J. Costello,

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

[FR Doc. 2025–21452 Filed 11–26–25; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2025–0040]

Agency Information Collection Activities: 1670–0048: SAFECOM Nationwide Surveys Generic Clearance

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

ACTION: 30-Day notice of information collection; request for comment; this is a renewal of a previously approved information collection. OMB Control Number: 1670–0048.

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 September 25, 2025 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: Comments are encouraged and will be accepted until December 29, 2025. Submissions received after the deadline for receiving comments may not be considered.

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: Antonio Branham, *Antonio.Branham@mail.cisa.dhs.gov,*

SUPPLEMENTARY INFORMATION: In 2006, Congress passed Public Law 109–295, which included SEC. 671. EMERGENCY COMMUNICATIONS also known as the ''21st Century Emergency Communications Act of 2006'. The legislation established the Department of Homeland Security (DHS) Office of Emergency Communications, which was re-designated in 2018 as the Emergency Communications Division (ECD) within the Cybersecurity and Infrastructure Security Agency (CISA), to lead the development and implementation of a comprehensive approach to advancing national interoperable communications capabilities. The following responsibilities were established: 6 U.S.C. 571(c) which requires the DHS Secretary through the ECD Assistant Director to: (4) Conduct 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 natural disasters, acts of terrorism, and other man-made disasters; (13) develop and update periodically, as appropriate, a National Emergency Communications Plan (NECP) under section 572 of this title; (14) perform such other duties of the Department necessary to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and (15) perform other duties of the Department necessary to achieve the goal of and maintain and enhance interoperable emergency communications capabilities. 6 U.S.C. 572(a) requires the Secretary in cooperation with State, local, and tribal governments, Federal departments and agencies, emergency response providers, and the private sector, to develop not later than 180 days after the completion of the baseline assessment under section 573 of this title, and periodically update the NECP.

Lastly, 6 U.S.C. 573 requires the DHS Secretary to conduct an assessment of Federal, State, local, and tribal governments that defines the range of capabilities needed by emergency response providers and relevant government officials, assesses the current available capabilities to meet such communications needs; identify the gaps between such current capabilities and defined requirements; at least every five years. These authorities, in addition to DHS responsibilities through Executive Order 13618 in the area of national security/emergency providers' communications, require periodic reexamination of nationwide emergency communications capabilities.

To perform these statutory obligations, CISA seeks renewal of its PRA Generic Clearance to maintain flexibility in implementing surveys that are relevant to the current emergency communications environment. To meet the statutory requirements of 6 U.S.C. 573, ECD conducts the SAFECOM Nationwide Survey (SNS) to assess evolving capability needs and gaps and track progress against policy initiatives, status of strategic plans, and major industry or market shifts affecting the emergency communications capability.

The purpose of the SNS is to gather information to assess available emergency communications capabilities and identify gaps and needs for emergency response providers to effectively communicate during all types of natural or man-made hazards. CISA ECD uses this information to complete its statutorily mandated assessment and share the data with all stakeholders that have a role in emergency communications. In order to ascertain this information, the SNS is comprised of a battery of instruments designed and distributed to emergency response disciplines at the federal, state/territorial, tribal, and local (county and municipal) levels of government, as well as the private sector. Methods of administration (questionnaire or interview) and distribution (online web form distributed via email or print forms