(NIMS) Incident Command System (ICS) and to provide hands-on exercises that reinforce the lecture materials. CISA and FEMA Emergency Management Institute (EMI) offer this course jointly as ''L0969, NIMS ICS All-Hazards Communications Unit Leader Course.'' Under the NIMS ICS structure, a COML is the focal point within the Communications Unit. This course provides DHS-approved and NIMS-compliant instruction to ensure that every state/territory has trained personnel capable of coordinating on-scene emergency communications during a multi-jurisdictional response or planned event.

The COMT course provides introductory and refresher training for the NIMS ICS COMT position. It introduces public safety professionals and support staff to various communications concepts and technologies including interoperable communications solutions, LMR communications, satellite, telephone, data, and computer technologies used in incident response and planned events. It is designed for state/territory, tribal, urban, and local emergency response professionals and support personnel in all disciplines who have a technical communications background. Participants develop the essential core competencies required for performing the duties of the COMT in an all-hazards incident, including responsibilities while operating in a local, regional, or state-level All-Hazards Incident Management Team.

In 2018 and 2019, ICTAP introduced the ITSL course, and SAFECOM/National Counsel of Statewide Interoperability Coordinators (NCSWIC) have coordinated with FEMA National Integration Center (NIC) and other organizations focused on public safety communications to establish the best way to integrate the ITSL into the ICS. The ITSL is needed to provide information management, cybersecurity, and application management for the many critical incident/event related functions to include: Incident/Unified Command Post, Incident Communications Centers, and various tactical operations centers, joint information center (JIC), staging areas, and field locations. The ITSL course targets Federal, state/territory, tribal, urban, local, and emergency response professionals, and support personnel in all disciplines with a communications background and an aptitude for and extensive experience in information technology. Specifically, the training course provides an overview of the ITSL components including Communications/IT Help Desk or Unified Help Desk, IT Infrastructure Manager, Network Manager. It covers their roles and responsibilities and provides an in-depth overview with exercises for the ITSL's major functions, to include ensuring reliable and timely delivery of IT services to participating agencies and officials.

The ICTAP Training Survey will not collect any personal identifiable information (PII) from respondents (emergency communications stakeholders) of the survey. In collecting feedback regarding the ITSL, COML, and COMT courses, the survey will collect what state the respondent lives, where they took the course, did the course provide the information needed, should the course curriculum be updated, and any comments to improve the course material. The survey will encompass 10 questions regarding the former student's experience, anything that they liked, disliked, or something new that they would like to see incorporated into the refreshed class. It is estimated that it will take each participant 10 minutes to complete the training survey. For 300 respondents annually, the burden is 50 hours. To estimate the cost of this collection, CISA uses the mean hourly wage of ''All Occupations'' of $25.72. CISA then applies a load factor of 1.4597 to this average wage to obtain a fully loaded average hourly wage of $37.54. The total respondent cost burden for this collection is $1,877 (50 hours × $37.54).

Analysis

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

Title of Collection: Interoperable Communications and Technical Assistance Program (ICTAP) Training Survey.

OMB Control Number: 1670–NEW.

Frequency: Annually.

Affected Public: State, Local, Tribal, and Territorial Governments.

Number of Annualized Respondents: 300.

Estimated Time per Respondent: 10 Minutes.

Total Annualized Burden Hours: 50 hours.

Total Annualized Respondent Opportunity Cost: $1,877.16.

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

Total Annualized Government Cost: $4,082.67.

Samuel Vazquez,

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

[FR Doc. 2021–13107 Filed 6–22–21; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2020–0005]

1670–NEW: SAFECOM Nationwide Surveys Generic Clearance

AGENCY: Emergency Communications Division (ECD), 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 Emergency Communications Division (ECD) 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 a notice about this ICR, in the **Federal Register** on February 19, 2021 for a 60-day public comment period. In response, there were no comment received. 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 February 17, 2021 at 86 FR 9948. Comments are due by July 23, 2021.

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: Eric Runnels, 703–705–6279, *necp@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) 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 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, develop not later than 180 days after the completion of the baseline assessment under section 573 of this title, and periodically update, a National Emergency Communications Plan.

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 a continuous examination of nationwide emergency communications capabilities.

The frequency and complexity of emergencies are on the rise during a time when technology is advancing at a faster pace than any other time in history. In order to perform these statutory regulations, it is important to understand the continuously changing requirements of emergency response providers and government officials at all levels of government, evolving risks, and the public safety community's ability to integrate new technologies while also preparing for emergent technologies. As a result, CISA is seeking a PRA Generic Clearance to allow for flexibility in implementing surveys that are relevant to the current security environment.

To meet the statutory requirements of 6 U.S.C. 573, ECD conducts the SAFECOM Nationwide Survey every 5 years 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.

CISA ECD conducts a web-based survey entitled the SAFECOM Nationwide Survey, hereinafter referred to as the SNS. The purpose of the survey 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 the information collected to complete a statutorily mandated assessment and shares the data with all stakeholders that have a role in emergency communications. In order to ascertain this information, the SNS deploys four similar surveys across the nation to various emergency response disciplines at each level of government—federal, state, territorial, tribal, and local. The survey solicits responses regarding issues affecting the public safety community to determine a jurisdiction's level of operability, interoperability and continuity and thus their overall emergency communications capability level. CISA ECD analyzes the data collected from this general survey to identify major gaps and themes affecting emergency communications across levels of government. Additionally, this analysis informs the development of supplemental surveys tailored to specific needs across the public safety community, as well as future iterations of the Nationwide Baseline Communications Assessment (NCBA) and National Emergency Communications Plan (NECP).

The results from the most recent surveys led to major updates to the update of the NECP released in September 2019. The NECP sets strategic priorities for the entire Nation. Additionally, the current collection allowed CISA ECD to share reliable data with emergency communications partners at all levels of government which assists them with: (1) Statewide Communications Interoperability Plan (SCIP) development, (2) Threat and Hazard Identification Risk Analysis (THIRA) development, (3) state-level grant programs and guidance, (4) federal grant applications assistance, and (5) funding and resource sharing strategy development.

CISA ECD conducts SAFECOM supplemental surveys. The surveys can be conducted as focus groups, in-person interviews, web- and paper-based. CISA ECD uses the information collected to complete statutorily mandated requirements (6 U.S.C. 571(c), 572(a), and 573) and shares the data with all stakeholders with a role in emergency communications. In order to ascertain this information, the SAFECOM supplemental surveys deploy topic-specific or targeted surveys across the nation to various emergency response disciplines at each level of government: Federal, state, territorial, tribal, and local. The surveys solicit responses regarding targeted issues affecting all public safety, emergency response communities and/or specific subsets of the SNS population. CISA ECD analyzes the data collected from these supplemental surveys to identify changing requirements, mitigate risks, and inform the data collected from the 5-year Nationwide Survey.

ECD uses electronic submission to reduce the burden on respondents including web-based surveys and assessment tools, such as Survey Monkey. Its target audience—mainly first responders—is frequently interrupted, have variable schedules, and frequently work long hours. Electronic submission provides a more user-friendly interface, provides anonymity to the users, ensures the maximum response rate, eliminates paper, printing, and postage costs along with the need for data entry.

We will also utilize alternative submission methods for both the SNS and the supplemental surveys. An Adobe PDF-fillable form which can be returned via email to *sns@cisa.dhs.gov,* direct emails with questionnaires attached, an in-person surveys, focus-groups, and a paper copy that will be mailed directly to the respondent(s) requesting a hard copy. The paper copy can be returned either via a prepaid envelope, scanned and emailed to *sns@cisa.dhs.gov,* and/or faxed to CISA ECD. We anticipate that .5% of respondents will utilize these alternative submission methods.

Analysis

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

Title of Collection: SAFECOM Nationwide Surveys Generic Clearance.

OMB Control Number: 1670–NEW.

Frequency: Annually.

Affected Public: State, Local, Tribal, and Territorial Governments.

Number of Annualized Respondents: 8,398.

Estimated Time per Respondent: 0.5 hours.

Total Annualized Burden Hours: 4,199 hours.

Total Annualized Respondent Opportunity Cost: $168,298.74.

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

Total Annualized Government Cost: $235,863.

Samuel Vazquez,

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

[FR Doc. 2021–13111 Filed 6–22–21; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2021–0009]

Revision of a Currently Approved Information Collection for the Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS.

ACTION: 60-Day notice and request for comments; revision of information collection request: 1670–0029.

Authority: 6 U.S.C. 621–629.

SUMMARY: The Infrastructure Security Division (ISD) within the Cybersecurity and Infrastructure Security Agency (CISA) is issuing a 60-day notice and request for comments to revise Information Collection Request (ICR) 1670–0029. CISA will submit the ICR to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are due August 23, 2021.

ADDRESSES: You may submit comments, identified by docket number CISA–2021–0009 through the Federal eRulemaking Portal available at *http://www.regulations.gov.* Follow the instructions for submitting comments.

Instructions: All comments received via *https://www.regulations.gov* will be posted to the public docket at *https://www.regulations.gov,* including any personal information provided.

Do not submit comments that include trade secrets, confidential commercial or financial information, Chemical-terrorism Vulnerability Information (CVI), Protected Critical Infrastructure Information (PCII), or Sensitive Security Information (SSI) directly to the public regulatory docket. Contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section below with questions about comments containing such protected information. CISA will not place comments containing such protected information in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. Additionally, CISA will hold them in a separate file to which the public does not have access and place a note in the public docket that CISA has received such protected materials from the commenter. If CISA receives a request to examine or copy this information, CISA will treat it as any other request under the Freedom of Information Act (FOIA).

FOR FURTHER INFORMATION CONTACT: Lona Saccomando, 202–579–0590, *CISARegulations@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The CFATS Program identifies chemical facilities of interest and regulates the security of high-risk chemical facilities through a risk-based approach. The CFATS Program is authorized under the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 [1] or ''CFATS Act of 2014''. CISA collects necessary information through 1670–0029 to implement the CFATS Personnel Surety Program.

Program Description

High-risk chemical facilities regulated by CISA under the CFATS Program must submit a Site Security Plan (SSP) or an Alternative Security Program (ASP) that describes how they will meet or exceed 18 risk-based performance standards (RBPS), including RBPS 12—Personnel Surety. Under RBPS 12, high-risk chemical facilities regulated under CFATS are required to account for the conduct of certain types of background checks in their Site Security Plans. Specifically, RBPS 12 requires high-risk chemical facilities to:

> Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including, (i) Measures designed to verify and validate identity; (ii) Measures designed to check criminal history; (iii) Measures designed to verify and validate legal authorization to work; and (iv) Measures designed to identify people with terrorist ties[.]6 CFR 27.230(a)(12).

The first three aspects of RBPS 12 (checks for identity, criminal history, and legal authorization to work) are performed by the facility. The fourth aspect (*i.e.,* the check for terrorist ties) was implemented in December 2016 at Tier 1 and Tier 2 facilities.[2] In July of 2019 the Department implemented the CFATS Personnel Surety Program for all tiers.[3] A complete description of the CFATS Personnel Surety Program is provided in the July 2019 notice and

[1] The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (also known as the CFATS Act of 2014, Pub. L. 113–254) codified the CFATS program into the Homeland Security Act of 2002. See 6 U.S.C. 621 *et seq.,* as amended by Public Law 116–136, Sec. 16007 (2020).

[2] The initial notice of implementation was published on December 18, 2015 at 80 FR 79058 and may be viewed at *https://www.federalregister.gov/d/2019-14591.*

[3] The notice of implementation at all high-risk chemical facilities was published on July 9, 2019 at 84 FR 32768 and may be viewed at *https://www.federalregister.gov/d/2019-14591.*