Estimated Time per Respondent: 0.083 hours (5 minutes).

Total Burden Hours: 41.7 annual burden hours.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Total Burden Cost: $3,576.

Instrument: Top-Screen Update.

Frequency: ''On occasion'' and ''Other.''

Affected Public: Business or other for-profit.

Number of Respondents: 2,500 respondents.

Estimated Time per Respondent: 0.083 hours (5 minutes).

Total Burden Hours: 312.5 hours.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Total Burden Cost: $26,818.

Instrument: Compliance Assistance.

Frequency: ''On occasion'' and ''Other.''

Affected Public: Business or other for-profit.

Number of Respondents: 1,600 respondents.

Estimated Time per Respondent: 0.083 hours (5 minutes).

Total Burden Hours: 133.3 annual burden hours.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Total Burden Cost: $11,443.

Instrument: Declaration of Reporting Status.

Frequency: ''On occasion'' and ''Other.''

Affected Public: Business or other for-profit.

Number of Respondents: 100 respondents.

Estimated Time per Respondent: 0.25 hours.

Total Burden Hours: 25 annual burden hours.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Total Burden Cost: $2,145.

Samuel Vazquez,

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

[FR Doc. 2021–13106 Filed 6–22–21; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2020–0018]

Agency Information Collection Activities: Proposed Collection; Comment Request; Cybersecurity and Infrastructure Security Agency (CISA) Visitor Request Form

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

ACTION: 30-Day Notice and request for comments; reinstatement without change of information collection request: 1670–0036.

SUMMARY: The Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Office of Compliance and Security (OCS), as part of its continuing effort to reduce paperwork and respondent burden, invites the general public to take this opportunity to comment on a reinstatement, without change, of a previously approved information collection for which approval has expired. CISA will submit the following Information Collection Request 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 17, 2021, for a 60-day public comment period. There were no comments 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 9949. Comments must be submitted on or before 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 INFOTMATION CONTACT: For specific questions related to collection activities, please contact Michael Washington, 202–591–0713, *michael.washington@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: Public Law 107–296 The Homeland Security Act of 2002, Title II, recognizes the Department of Homeland Security role in integrate 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 Compliance and Security must maintain a robust visitor screening capability.

The CISA Office of Compliance and Security will collect, using an electronic form, information about each potential visitor to CISA facilities and the nature of each visit. The Office of Compliance and Security will use collected information to make a risk-based decision to allow visitor access to CISA facilities.

This proposed information collection previously published in the **Federal Register** on February 17, 2021, at 86 FR 9949 with a 60 day public comment period. No relevant comments were received. This information collection expired on February 28, 2021. CISA is requesting a reinstatement, without change, of a previously approved information collection for which approval has expired. 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: Cybersecurity and Infrastructure Security Agency (CISA) Visitor Request Form.

OMB Control 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 Respondent Opportunity Cost: $125,144.

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

Total Government Cost: $250,473.

Samuel Vazquez,

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

[FR Doc. 2021–13109 Filed 6–22–21; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2020–0020]

ICTAP Training Survey

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 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 19, 2021 at 86 FR 10332. Comments are encouraged and will be accepted until 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: For specific questions related to collection activities, please contact John Peterson *COMU@cisa.dhs.gov* at 202–503–5074.

SUPPLEMENTARY INFORMATION: The National Emergency Communications Plan (NECP) is the Nation's over-arching strategic plan to drive measurable improvements in emergency communications across all levels of government and disciplines. First released in 2008, the plan is periodically updated to reflect the ongoing evolution of emergency communications technologies and processes. In support of the NECP, the Interoperable Communications and Technical Assistance Program (ICTAP) within the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD) provides a portfolio of no-cost communications technical assistance (TA) to support the implementation of the NECP, state's and territories' Statewide Communication Interoperability Plans (SCIPs), broadband planning, voice and digital network engineering, training, exercise support, and operational assessment focused on interoperable emergency communications at all levels of government.

The purpose of the ICTAP Training Survey is to obtain anonymous feedback regarding several of the training courses offered by the ICTAP. The feedback and experience given by survey respondents will assist the ICTAP in improving, revising, and updating the course materials for future students. The three courses which the ICTAP would like to obtain feedback are for:

- Communications Unit Leader (COML);
- Communications Unit Technician (COMT); and
- Information Technology Service Unit Leader (ITSL).

COML is designed for all state/territory, tribal, regional, and local emergency response professionals and for support personnel with a communications background. It is designed to familiarize these professionals with the role and responsibilities of a COML under the National Incident Management System (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.

COML is designed for all state/territory, tribal, regional, and local emergency response professionals and for support personnel with a communications background. It is designed to familiarize these professionals with the role and responsibilities of a COML under the National Incident Management System