DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA- CISA-2022-0012]

Agency Information Collection Activities: Incident Communications Activity Report (ICAR)

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

ACTION: 30- Day Notice and request for comments; New collection (Request for a new OMB Control Number, 1670-NEW.

SUMMARY: The Emergency Communications Division (ECD within the Cybersecurity and Infrastructure Security Agency (CISA) is issuing a 30-day notice and request for comments to for 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.

DATES: Comments are encouraged and will be accepted until [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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: Wes Rogers, 202-897-8132, wes.rogers@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: CISA previously published this information collection request (ICR) in the *Federal Register* on OCTOBER 20, 2022 for a 60-day public comment period. One comment was received from the Cellular Telecommunications Industry Association (CTIA) during the 60 Day FRN comment period for the Incident Communications Activity Report. The response to this comment has been addressed within the contents of this 30-DAY FRN. The purpose of this notice is to allow additional 30-days for public comments.

The Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD) is mandated by The Cybersecurity and Infrastructure Security Act of 2018, 6 U.S.C. 652(f) under Sections (9) carry out emergency communications responsibilities, in accordance with sub-chapter XIII; (10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector Risk Management Agencies, as appropriate; and (11) provide education, training, and capacity development to Federal and non-Federal entities to

enhance the security and resiliency of domestic and global cybersecurity and infrastructure security;.

This information collection is requested to be completed by ECD stakeholders—including state and local emergency communications professionals—through The Incident Communications Activity Report (ICAR) form. The ICAR was developed with the intention of capturing and documenting the emergency communications activity and utilization of public safety communications technologies controlled by state or local emergency response officials organized to provide command and coordination for an incident, planned event, or exercise. As a result, CISA/ECD seeks to execute a standard request from the Paper Reduction Act (PRA) to review, analyze, and revise current Incident Communication Activity.

The Emergency Communications Division (ECD) is a division within the Cybersecurity and Infrastructure Security Agency (CISA) which serves under the direction of the Department of Homeland Security (DHS). ECD coordinates with National Security and Emergency Preparedness (NS/EP) communications stakeholders to enable use of technical assistance and information sharing to reduce communications system impacts or vulnerabilities. CISA has authority to perform assessments and evaluations for federal and non-federal entities, with consent and upon request. CISA leverages several different authorities, including but not limited to Presidential Policy Directive – 21 (PPD-21), the National Infrastructure Protection Plan (NIPP) Voluntary Partnership Framework, and Sec. 871 of the Homeland Security Act of 2002 to fullfill the Department's responsibility to

> "[c]onduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the Sector Rick Management Agencies and in collaboration with SLTT [State, Local, Tribal, and Territorial] entities and critical infrastructure owners and operators."

The one comment CISA received is from CTIA - The Wireless Association® ("CTIA") (), which represents the U.S. wireless communications industry and companies

throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers, as well as apps and content companies. CTIA advocates for government policies that foster continued wireless innovation and investment. CTIA's comment states:

> "CISA should refrain from directing state and local public safety officials from opining on the general availability of commercial "cellular" services during a disaster event through Incident Communications Activity Reports."

The ICAR does not collect information regarding any system availability, therefore it does not collect information regarding commercial system availability or performance. As a result, the 30-day FRN does not include the previous identification of public safety communications technologies and has also been updated within all applicable areas to read:

> "emergency communications activity and utilization of public safety communications technologies controlled by state or local emergency response officials."

The information collected will provide on-the-ground data on emergency communications activity and utilization of public safety communications technologies controlled by state or local emergency response officials organized to provide command and coordination for an incident, planned event, or exercise.

The information captured focuses on a number of key areas: incident complexity, command and coordination systems, and all-hazards information and communications technology positions, resources (*e.g.* voice and data systems, interoperability techniques, and planning references), challenges and general conditions encountered during the incident.

ICAR will be submitted electronically by the emergency responder with overall information and communications technology responsibilities within the identified command and coordination organization, for a reporting period.

This information will inform other jurisdictions on best practices while permitting data-driven decisions on future policy improvements. CISA, in support of the National Council of Statewide Interoperability Coordinators (NCSWIC) and the CISA interoperable-communications program known as SAFECOM, will collect data through a two-page report to capture the emergency communications activity and utilization of public safety communications technologies controlled by state or local emergency response officials organized to provide command and coordination for an incident, planned event, or exercise.

CISA's goal is to identify lessons learned to drive strategy and improve existing or offer new technical assistance within the scope of emergency communications activity for Incidents, Planned Events, or Exercises. The ICAR is completed by the person with overall information and communications technology responsibilities with the identified command and coordination organization, for the indicated reporting period.

The reporting period is flexible to meet agency or jurisdictional program needs. The report is designed to accommodate a single report for the incident or event duration, or multiple reports for smaller time periods within the same incident or event. State, local, territorial, or tribal incident communications organizational and technical challenges and best practices will be captured. Collecting and summarizing this data will drive our nationwide response, drive strategy, and goal development—subsequently improving existing and/or offer new Technical Assistance options to stakeholders.

The ICAR is an electronically submitted form to populate the data sets which will be loaded, stored, and analyzed in the Division's data analytics system. Electronic data collection enables an efficient and straightforward submission process to submit, reducing the time and effort for the submitter while also reducing errors.

ICAR form is voluntarily submitted using a Microsoft Teams Form link. The ICAR form will require a total effort of approximately five minutes for completion. The

ICAR form will be completed per incident. Leveraging the MS Forms and a fillable PDF there will be no printing of forms needed, no preparing and sending emails or memos per incident. Participants will be able to input free form information in addition to drop down type questions.

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: Incident Communications Activity Report (ICAR)

OMB Number: 1670-NEW

Frequency: per incident on a voluntary basis

Affected Public: State, Local, territorial and Tribal public safety communications personnel

Number of Respondents: 450

Estimated Time Per Respondent: 0.083 hours

Total Burden Hours: 37.5 hours

Total Burden Cost (capital/startup): $0

Total Burden Cost (operating/maintaining): $2,131.15

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

[FR Doc. 2023-19103 Filed: 9/1/2023 8:45 am; Publication Date: 9/5/2023]