9110-9P P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2022-0012]

Incident Communications Activity Report (ICAR)

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

ACTION: 60-day notice and request for comments; new collection (request for a new OMB Control Number, 1670-NEW.

SUMMARY: DHS CISA Emergency Communications Division (ECD) 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.

DATES: Comments are encouraged and will be accepted until [***INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER***].

ADDRESSES: You may submit comments, identified by docket number CISA-2022-0012, by one of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Please follow the instructions for submitting comments.
- Mail: CISA strongly prefers comments to be submitted electronically. Written comments and questions about this Information Collection Request should be forwarded to CISA/ECD, ATTN Mark Carmel: CISA - Mailstop 0612, Cybersecurity and Infrastructure Security Agency, 4200 Wilson Blvd, Arlington, VA 20598-0612.

Instructions: All submissions received must include the words "Department of Homeland Security" and a corresponding 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 confidential comments, such as sensitive personal information or proprietary information. 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 Wes Rogers at 202-897-8132 or at wes.rogers@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: 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 of any organized incident management command and coordination structure established 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. This authority is consistent with 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 information collected will provide on-the-ground data on emergency communications activity of any organized incident management command and coordination structure established 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 Counsel 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 of any organized incident management command and coordination structure established 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 communications and public safety technologies communications challenges and best practices will be captured. Public safety communications technologies would include – Cellular, Tactical Information Technology, Emergency Alert Systems, Land Mobile Radio, Satellite, 9-1-1 and emergency communications centers. Collecting and summarizing this data will drive our nationwide response, drive strategy, and goal development—subsequently improving existing and/or offer new Technical Assistance option 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.

We will send the ICAR form out using a Microsoft Teams Form link via email. The ICAR form will require a total effort of approximately five minutes for completion. The ICAR form will be completed per incident. The recipients are individuals we deal with on a regular basis and are in constant contact with them. 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 a couple drop down type questions which will be asked.

This is a **NEW** of an information collection.

OMB is particularly interested in comments that:

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
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: Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

Title of Collection: Incident Communications Activity Report (ICAR).

OMB Control Number: 1670-NEW.

Frequency: per incident on a voluntary basis.

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

Number of Annualized Respondents: 450.

Estimated Time Per Respondent: 0.083 hours.

Total Annualized Burden Hours: 37.5 hours.

Total Annualized Respondent Opportunity Cost: $2,131.15.

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

Total Annualized Government Cost: $25,563.

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

[FR Doc. 2022-22791 Filed: 10/19/2022 8:45 am; Publication Date: 10/20/2022]