Estimated Total Annual Cost to the Federal Government: $6,153,716.

Comments

Comments may be submitted as indicated in the **ADDRESSES** caption above. Comments are solicited to (a) evaluate whether the proposed data collection is necessary for the proper performance of the agency, including whether the information shall have practical utility; (b) 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; (c) enhance the quality, utility, and clarity of the information to be collected; and (d) 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 submission of responses.

Millicent Brown Wilson,

Records Management Branch Chief, Office of the Chief Administrative Officer, Mission Support, Federal Emergency Management Agency, Department of Homeland Security.

[FR Doc. 2022–24066 Filed 11–3–22; 8:45 am]

BILLING CODE 9111–78–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2022–0014]

Communications Assets Survey and Mapping (CASM) Tool

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

ACTION: 60-Day notice and request for comments; extension without change of a currently approved collection request: 1670–0043.

SUMMARY: CISA is issuing a 60-day notice and request for comments to extend use of Information Collection Request (ICR) 1670–0043. 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 encouraged and will be accepted until January 3, 2023.

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 DHS/CISA/ECD, ATTN: 1670–NEW, 245 Murray Lane SW, Mail Stop 0640, Kendall Carpenter, Arlington VA 20528.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the 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 in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an email comment, your email address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. 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 Steven Singer at 202–499–0289 or at *steven.singer@cisa.dhs.gov*.

SUPPLEMENTARY INFORMATION: The CISA ECD, formed under Title XVIII of the Homeland Security Act of 2002, 6 U.S.C. 571 *et seq.,* as amended, is required to develop and maintain the Nationwide Emergency Communications Plan (NECP). The vision of the NECP is to ensure emergency response personnel can communicate as needed, on demand, and as authorized. To achieve this vision, ECD provides the Communications Assets and Survey Mapping (CASM) Tool. The CASM Tool is the primary resource nationwide for the emergency communications community to inventory and share asset and training information for the purpose of planning public safety communications operability and interoperability.

ECD provides the CASM Tool as a secure and free nationwide database to contain communications capabilities for use by Federal, State, Local, Territorial, and Tribal (SLTT) emergency personnel. CASM allows Federal employees and SLTT Statewide Interoperability Coordinators (SWIC) to inventory emergency communication equipment and resources. The information entered is voluntary and used by SWIC to support tactical planning and coordination during emergencies. ECD does not utilize the information entered into CASM. ECD only provides, maintains, and stores the information entered in the CASM database and only has administrative access to the information entered. All information is collected via electronic means. The CASM registration and database tool is available online via *https://casm.dhs.gov/.* Users can also access and enter information via the CASM Resource Finder mobile app.

This is an *EXTENSION* of a current approved information collection without change.

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

Title of Collection: Communications Assets Survey and Mapping Tool.

OMB Control Number: 1670–0043.

Frequency: Annually.

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

Number of Annualized Respondents: 56.

Estimated Time per Respondent: 5 minutes (0.08 hours) per registration or 30 minutes (0.50 hours) for tool modules.

Total Annualized Burden Hours: 341 hours.

Total Annualized Respondent Opportunity Cost: $16,215.

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

Total Annualized Government Cost: $3,000,000.

Robert Costello,

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

[FR Doc. 2022–23987 Filed 11–3–22; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2022–0050]

Homeland Security Advisory Council

AGENCY: The Department of Homeland Security (DHS), The Office of Partnership and Engagement (OPE).

ACTION: Notice of new taskings for the Homeland Security Advisory Council (HSAC).

SUMMARY: On October 16, 2022 the Secretary of DHS, Alejandro N. Mayorkas, tasked the Homeland Security Advisory Council (HSAC) to establish four new subcommittees further outlined below. This notice is not a solicitation for membership.

FOR FURTHER INFORMATION CONTACT: Rebecca Sternhell, Executive Director of the Homeland Security Advisory Council, Office of Partnership and Engagement, U.S. Department of Homeland Security at *HSAC@hq.dhs.gov* or 202–891–2876.

SUPPLEMENTARY INFORMATION: The HSAC provides organizationally independent, strategic, timely, specific, and actionable advice and recommendations for the consideration of the Secretary of the Department of Homeland Security on matters related to homeland security. The HSAC is comprised of leaders in local law enforcement, first responders, public health, State, local and tribal government, national policy, the private sector, and academia.

The four new subcommittees are as follows:

Subcommittee (1): DHS Leadership in Supply Chain Security

A subcommittee to provide recommendations on how the Department can take a greater leadership role in supply chain security, including by strengthening supply chain cybersecurity.

Subcommittee (2): DHS Intelligence and Information Sharing

A subcommittee to provide recommendations on how the Department can improve upon its intelligence and information sharing with our key federal, state, local, tribal, territorial, and private sector partners. The subcommittee will assess whether the Department's information sharing architecture developed by the DHS Office of Intelligence and Analysis (I&A) is adequate for the threats of today and tomorrow, and provide advice and recommendations to better enable the Office of Intelligence and Analysis (I&A) to rapidly and efficiently share information and intelligence with our key partners.

Subcommittee (3): DHS Transparency and Open Government

A subcommittee to provide recommendations on how the Department can improve its commitment to transparency and open government. The subcommittee will provide advice and recommendations that will position the Department as the leader in this critical area of model government conduct.

Subcommittee (4): Homeland Security Technology and Innovation Network

A subcommittee to provide recommendations on how the Department can create a more robust and efficient Homeland Security Technology and Innovation Network. The subcommittee will provide advice and recommendations that will develop the Department's innovation, research and development, and technology network with the private sector.

Tasking (1): DHS Leadership in Supply Chain Security

The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. DHS continues to protect America's national and economic security by facilitating legitimate trade and travel and rigorously enforcing U.S. customs and immigration laws and regulations.

As the Department strives to stay ahead of the curve and take a greater leadership role by harnessing new technologies, minimizing environmental impact, and increasing partnerships in this vital area, this HSAC subcommittee is tasked to provide recommendations on how the Department can take a greater leadership role in supply chain security. The subcommittee's assessment will include, but need not be limited to, the following:

a. strengthening physical security;

b. strengthening cybersecurity; and,

c. increasing efficiencies to ensure a resilient, safe, and secure supply chain for critical manufacturing and technology sectors.

Tasking (2): DHS Intelligence and Information Sharing

Federal, state, local, tribal, and territorial partners convened shortly after the September 11, 2001 terrorist attacks, creating a domestic information sharing architecture to enable the timely and seamless exchange of information to detect and eliminate terrorist threats. In the 21 years since 9/11, our law enforcement and homeland security community has made great progress in reshaping our information sharing environment. Working together, we put policies and processes in place that help us to be safer and more secure than we were years ago.

As the Department approaches its 20th Anniversary, the HSAC subcommittee is asked to provide recommendations on:

1. How the Department can rapidly and efficiently share intelligence and information with its federal, state, local, tribal, territorial, and private sector partners. Have DHS investments in information sharing technology and changes in law and policy resulted in increased knowledge transfer and resilience? Are further investments or changes in law or policy needed?

2. Has DHS created an information and intelligence sharing architecture that efficiently spreads knowledge and rapidly shares critical information? Are there steps that we need to take to revitalize or improve this architecture?

3. Whether the current DHS information sharing architecture optimizes information sharing for threats other than counterterrorism; for example, cyber, border security, foreign influence/propaganda, strategic advantage, and others.

4. Internal DHS Information Sharing: Has DHS fully implemented internal DHS information sharing policy—for example, the One DHS Memo—to leverage DHS data and information to support Departmental missions like border security as well as to develop and share relevant, quality intelligence with our partners?

Tasking (3): DHS Transparency and Open Government

DHS is committed to transparency and promoting the principles of an Open Government. The United States has worked both domestically and internationally to ensure global support for Open Government principles to promote transparency, fight corruption, energize civic engagement, and leverage new technologies in order to strengthen