There will be a public comment period from approximately 3 p.m. until 3:15 p.m. (EST). Speakers are requested to limit their comments to 3 minutes. Please note that the public comment period may end before the period allotted, following the last call for comments. Please contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section above to register as a speaker.

Dated: December 6, 2023.

**Amy M. Beach,**

*Captain, U.S. Coast Guard, Director of Inspections and Compliance.*

[FR Doc. 2023–27169 Filed 12–11–23; 8:45 am]

**BILLING CODE 9110–04–P**

## DEPARTMENT OF HOMELAND SECURITY

### Federal Emergency Management Agency

**[Docket ID: FEMA–2023–0034; OMB No. 1660–NW172]**

### Agency Information Collection Activities: Proposed Collection; Comment Request; Generic Clearance for FEMA's Preparedness Grant Programs

**AGENCY:** Federal Emergency Management Agency, Department of Homeland Security.

**ACTION:** 60-Day notice of new collection and request for comments.

**SUMMARY:** The Federal Emergency Management Agency (FEMA), as part of its continuing effort to reduce paperwork and respondent burden, invites the general public to take this opportunity to comment on a new information collection. In accordance with the Paperwork Reduction Act of 1995 (PRA), this notice seeks comments concerning a new generic collection to oversee FEMA's Office of Grants Administration programmatic and financial stewardship of non-disaster grant awards.

**DATES:** Comments must be submitted on or before February 12, 2024.

**ADDRESSES:** To avoid duplicate submissions to the docket, please submit comments at *www.regulations.gov* under Docket ID FEMA–2023–0034. Follow the instructions for submitting comments.

All submissions received must include the agency name and Docket ID.

Regardless of the method used for submitting comments or material, all submissions will be posted, without change, to the Federal eRulemaking Portal at *http://www.regulations.gov,* and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to read the Privacy and Security Notice that is available via a link on the homepage of *www.regulations.gov.*

**FOR FURTHER INFORMATION CONTACT:** Amy Bulgrien, Senior Advisor, FEMA, Office of Grants Administration at *amy.bulgrien@fema.dhs.gov* and 202–880–7522. You may contact the Information Management Division for copies of the proposed collection of information at email address: *FEMA-Information-Collections-Management@fema.dhs.gov.*

**SUPPLEMENTARY INFORMATION:** FEMA's Office of Grants Administration was created to oversee the programmatic management, financial management and administration of non-disaster grants. These programs help make the country more resilient and support the Nation's needs before, during, and after disasters. Non-disaster grants also help develop and sustain capabilities at the state, local, Tribal, and territorial levels to mitigate, prevent, protect against, respond to, and recover from terrorism or other high-consequence disasters and emergencies. The instruments in this collection are required to apply for FEMA funds and the data collected through these instruments is used by FEMA to evaluate grant applications, assess applicant risk, monitor awards for compliance, and comply with Federal laws and regulations. OGA manages and ensures accountability of FEMA preparedness grant programs under sections 430, 503(b)(2)(G), 504(a)(12), 2021–2023, and 2220–A of the Homeland Security Act of 2002. OGA programmatically manages and financially administers certain non-disaster and preparedness grants and conduct environmental planning and historic preservation activities for these grants, including homeland security and preparedness grants (including statutory authority for certain waivers) pursuant to titles V, XVIII, and XX of the Homeland Security Act of 2002; section 503(b)(2)(B), (G), and (H) of the Homeland Security Act of 2002 (6 U.S.C. 313(b)(2)(B), (G), and (H)); section 1809 of the Homeland Security Act of 2002 (6 U.S.C. 579); titles XIV and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007; 46 U.S.C. 70107; sections 635 and 662 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 723 and 762); title VI of the Stafford Act, as amended; Reorganization Plan No. 3 of 1978, 5 U.S.C. app.; sections 33 and 34 of the Federal Fire Prevention and Control Act of 1974, as amended (15 U.S.C. 2229, 2229a); section 3006 of the Deficit Reduction Act of 2005, as amended; section 204 of the REAL ID Act of 2005; the Coronavirus Aid, Relief, and Economic Security Act, Div. B (Pub. L. 116–136); and grant programs authorized in annual appropriations acts or future preparedness grant program authorities.

FEMA's Office of Grants Administration is submitting this request for a generic collection to streamline integration of stakeholder feedback on instruments. This collection will ensure all Office of Management and Budget (OMB) control number expiration dates are aligned across the OGA portfolio.

**Collection of Information**

*Title:* Generic Clearance for FEMA's Preparedness Grant Programs.

*Type of Information Collection:* New Collection.

*OMB Number:* 1660–NW172.

*FEMA Forms:* Not Applicable.

*Abstract:* FEMA's Office of Grants Administration was created to oversee the programmatic management, financial management, and administration of non-disaster grants. Non-disaster grant programs help make the country more resilient and support the nation's needs before, during, and after disasters. Non-disaster grants help develop and sustain capabilities at the state and local, tribal, and territorial levels to mitigate, prevent, protect against, respond to, and recover from terrorism or other high-consequence disasters and emergencies. Instruments in this collection are required to apply for FEMA funds; data collected via the instruments is used by FEMA to evaluate grant applications, assess applicant risk, monitor awards for compliance, and comply with Federal laws and regulations.

*Affected Public:* State, Local or Tribal Government; Businesses or other For-profits; Not-for Profit institutions.

*Estimated Number of Respondents:* 35,552.

*Estimated Number of Responses:* 55,244.

*Estimated Total Annual Burden Hours:* 1,737,291.

*Estimated Total Annual Respondent Cost:* $100,067,963.

*Estimated Respondents' Operation and Maintenance Costs:* $0.

*Estimated Respondents' Capital and Start-Up Costs:* $0.

*Estimated Total Annual Cost to the Federal Government:* $3,090,494.

**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. 2023–27196 Filed 12–11–23; 8:45 am]

**BILLING CODE 9111–23–P**

## DEPARTMENT OF HOMELAND SECURITY

### Agency Information Collection Activities: ReadySetCyber Initiative Questionnaire

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

**ACTION:** 30-Day notice and request for comments; request for a new OMB control number, 1670–NEW.

**SUMMARY:** The Cyber Security Division's Vulnerability Management Sub-Division 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. CISA previously published this information collection request in the **Federal Register** on August 10, 2023 for a 60-day public comment period. 0 comments were received by CISA. The purpose of this notice is to allow additional 30 days for public comments.

**DATES:** Comments are encouraged and will be accepted until January 11, 2024.

**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:** Mark Robinson, 202–740–6114, *mark.robinson@hq.dhs.gov.*

**SUPPLEMENTARY INFORMATION:** Consistent with CISA's authorities to ''carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States'' at 6 U.S.C. 652(e)(1)(B) and provide Federal and non-Federal entities with ''operational and timely technical assistance'' at 6 U.S.C. 659(c)(6) and ''recommendation on security and resilience measures'' at 6 U.S.C. 659(c)(7), CSD VM's ReadySetCyber initiative will collect information in order to provide tailored technical assistance, services and resources to critical infrastructure organizations from all 16 critical infrastructure sectors based on the maturity of their respective cybersecurity programs.

CISA seeks to collect this information from US critical infrastructure organizations on a strictly voluntary and fully electronic basis so that each organization can be best supported in meeting the CISA Cybersecurity Performance Goals. The CISA Cybersecurity Performance Goals are a set of 38 voluntary controls which aim to reduce the risk of cybersecurity threats to critical infrastructure.

CISA offers a number of services and resources to aid critical infrastructure organizations in adopting the Cybersecurity Performance Goals and seeks to make discovery of the appropriate services and resources as easy as possible, especially for organizations that many have cybersecurity programs at low levels of capability. For example, an organization that is unsure of its ability to enumerate all its assets with Internet Protocol addresses can leverage CISA's highly scalable vulnerability scanning service to discover additional assets within its network range that may have been previously unknown. Organizations with more mature cybersecurity programs who wish to evaluate their network segmentation controls will be better positioned to take advantage of CISA's more resource-intensive architecture assessments.

To measure adoption of the Cybersecurity Performance Goals and assist organizations in finding the best possible services and resources for their cybersecurity programs, CISA is seeking to establish a voluntary information collection that uses respondents' answers to tailor a package of services and resources most applicable for their level of program maturity.

Without collecting this information, CSD VM will be unable to tailor an appropriate suite of services, recommendations, and resources to assist that organization in protecting itself against cybersecurity threats, thereby creating burdens of inefficiency for service requesters and CSD VM alike. In addition, this information is critical to CSD VM's ability to measure the adoption of CISA's Cybersecurity Performance Goals by critical infrastructure organizations and assess the maturity of critical infrastructure organizations' cybersecurity programs.

The information to be collected includes: Identity and access management, device configuration and security, date security, governance and training, vulnerability management, supply chain risk management, and incident response.

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;