and Infrastructure Security Agency (CISA) submits the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review. CISA previously published this ICR in the **Federal Register** on February 29, 2024, for a 60-day public comment period. One comment was received by CISA. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until September 19, 2025.

Submissions received after the deadline for receiving comments may not be considered.

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: If additional information is required contact: Christopher Murray, 202–984–0874, *christopher.murray@mail.cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The Cybersecurity and Infrastructure Security Agency (CISA) operates the federal information security incident center. Through this center, CISA provides technical assistance and guidance on detecting and handling security Vulnerability Disclosures, compile and analyze incident information that threatens information security, inform agencies of current and potential threats and vulnerabilities, and provide intelligence or other information about cyber threats, vulnerabilities, and incidents to agencies. 44 U.S.C. 3556(a), see also 6 U.S.C. 659(c) (providing for cybersecurity services for both Federal Government and non-Federal Government entities).

CISA is responsible for performing coordinated Vulnerability Disclosure, which may originate outside the United States Government (USG) network/community and affect users within it or originate within the USG community and affect users outside of it. Often, therefore, the effective handling of security incidents relies on information sharing among individual users, industry, and the USG, which may be facilitated by and through CISA. A dedicated form on the CISA website will allow for external reporting of vulnerabilities that the reporting entity believes to be Known Exploited Vulnerabilities (KEV) eligible. Upon submission, CISA will evaluate the information provided, and then will add to the KEV Catalog, if all KEV requirements are met. For the digital copy of this information collection for review, please contact the POC listed above in this notice request.

CISA received one comment (which didn't speak to any of salient aspects of the information collection) during the open window period that said ''I am curious to learn more about this process as my team has built the world's premier exploit and vulnerability intelligence dataset—and we do track our own known exploited vulnerabilities and are looking at methods to coordinate with CISA KEV team.'' CISA replied with the following information:

''The intent of this form is to allow members of the public (vendors, researchers, essentially anyone) to propose vulnerabilities to CISA that they feel meet the CISA Known Exploited Vulnerabilities (KEV) requirements. These requirements are outlined on the CISA KEV website: *https://www.cisa.gov/known-exploited-vulnerabilities.* Once the user submits the form, our CISA KEV Team is notified and then we triage the information provided. If it does not meet all requirements, we then use the provided information as a starting point, and we do our own research to see if we can find additional information to meet all three requirements. If we do have all required information, we then proceed with adding the vulnerability to the CISA KEV Catalog. I [have] attached the proposed layout of the webform. While the form will not include any additional questions, the verbiage itself is subject to change based on all required approvals.''

Analysis

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

Title: Actively exploited Vulnerability Submission Form.

OMB Number: 1670–NEW.

Frequency: Per incident on a voluntary basis.

Affected Public: State, local, Territorial, and Tribal, International, private sector partners.

Number of Respondents: 2,725.

Estimated Time per Respondent: 0.167 hours.

Total Burden Hours: 454 hours.

Total Annual Burden Cost: $37,956.

Total Government Burden Cost: $145,924.

Robert J. Costello,

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

[FR Doc. 2025–15888 Filed 8–19–25; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Vulnerability Reporting Submission Form

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

ACTION: 30-day notice and request for comments; new information collection request and OMB 1670–NEW.

SUMMARY: The Vulnerability Management (VM) subdivision within Cybersecurity and Infrastructure Security Agency (CISA) submits 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 this ICR in the **Federal Register** on October 30, 2024, for a 60-day public comment period. CISA received one comment. The purpose of this notice is to allow an additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until September 19, 2025.

Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: Written comments 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: If additional information is required contact: Kevin Donovan, 202–505–6441, *kevin.donovan@mail.cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The Cybersecurity and Infrastructure Security Agency (CISA) operates Coordinated Vulnerability Disclosure (CVD) in partnership with industry stakeholders and community researchers alike. Through this collaboration, CISA provides technical assistance and guidance on detecting and handling security Vulnerability Disclosures, compiles, and analyzes incident information that may threaten information security. 6 U.S.C. 659(c)(1), see also 6 U.S.C. 659(c)(6) (providing for information sharing capabilities as the federal civilian interface for sharing of cybersecurity information and providing technical assistance and risk management support for both Federal Government and non-Federal Government entities). CISA is also authorized to carry out these CVD functions by 6 U.S.C. 659(n) on Coordinated Vulnerability Disclosure, which authorizes CISA to, in coordination with industry and other stakeholders, may develop and adhere to DHS policies and procedures for coordinating vulnerability disclosures.

CISA is responsible for performing Coordinated Vulnerability Disclosure, which may originate outside the United States Government (USG) network/community and affect users within the USG and/or broader community or originate within the USG community and affect users both within and outside of it. Often, therefore, the effective handling of security incidents relies on information sharing among individual users, industry, and the USG, which may be facilitated by and through CISA. A dedicated form on the CISA website will allow for reporting of vulnerabilities that the reporting entity believes to be CISA Coordinated Vulnerability Disclosure (CVD) eligible. Upon submission, CISA will evaluate the information provided, and then will triage through the CVD process, if all CISA scoped CVD requirements are met.

CISA received one comment during the 60-day comment period. The commentator provided comments on the reporting process and questioned the accuracy of the burden estimate to include the numbers and the terminology between the use of the word ''respondents'' as opposed to ''response.'' The same commentator inquired as to what amount of preparation if any is given to those who advise on vendor vulnerabilities.

CISA thanked the commentator on the feedback and analysis and clarified that CISA's Vulnerability Disclosure Submission Form is an effort to improve how CISA collects vulnerability information from the public. CISA explained that the form is designed to improve CISA's intake and triage capabilities and that the form builds upon existing processes and does not involve developing an entirely new or independent framework. As to the burden estimates, CISA explained that the estimates were derived from historical data and operational experience under CISA's existing vulnerability coordination efforts. CISA further noted the suggested term of ''responses'' instead of ''respondents'' may better reflect number of submissions rather than unique individuals is noted and indicated the change to be incorporated into future communications on the effort to ensure clarity.

Analysis

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

Title: Vulnerability Disclosure Submission Form.

OMB Number: 1670–NEW.

Frequency: Per report on a voluntary basis.

Affected Public: State, local, Territorial, and Tribal, International, Private Sector Partners.

Number of Respondents: 2,725.

Estimated Time Per Respondent: 0.167 hours.

Annualized Respondent Cost: $39,536.

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

Total Annualized Government Cost: $63,447.

Robert J. Costello,

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

[FR Doc. 2025–15887 Filed 8–19–25; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2025–0001]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Speaker Request Form

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

ACTION: 30-Day notice of information collection; request for comment; this is a extension of a previously approved information collection (1670–0047).

SUMMARY: The Office of the Chief External Affairs Officer (EA) within Cybersecurity and Infrastructure Security Agency (CISA) submits 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 (ICR) in the **Federal Register** on May 29, 2025 for a 60-day public comment period. Zero 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 September 19, 2025. Submissions received after the deadline for receiving comments may not be considered.

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