9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2024-0008]

Agency Information Collection Activities: Actively Exploited Vulnerability Submission Form

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

ACTION: 60-day notice and request for comments; new collection request and OMB Control number is 1670-NNEW.

SUMMARY: The Vulnerability Management (VM) 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.

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 Docket # CISA-2024-0008, at:

- Federal eRulemaking Portal: http://www.regulations.gov. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # CISA-2024-0008. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT:

Christopher Murray, christopher.murray@cisa.dhs.gov, or 202-984-0874.

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 believe 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 developmental digital copy of this information collection for review, please contact the POC listed above in this notice request.

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: 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

Annual Cost Burden: $37,956

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

Total Annualized Government Cost: $145,924

Robert J. Costello,
Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.
[FR Doc. 2024-04193 Filed: 2/28/2024 8:45 am; Publication Date: 2/29/2024]