Community	Community map repository address
Hays County, Texas and Incorporated Areas Project: 24–06–0079S Preliminary Date: March 25, 2025	
City of Buda	Development Services, 405 East Loop Street, Building 100, Buda, TX 78610.
City of Creedmoor	City Hall, 5008 Hartung Lane, Creedmoor, TX 78610.
City of Kyle	Building Department, 100 West Center Street, Kyle, TX 78640.
City of Niederwald	City Hall, 8807 Niederwald Strasse, Niederwald, TX 78640.
City of Uhland	City Hall, 15 North Old Spanish Trail, Uhland, TX 78640.
Unincorporated Areas of Hays County	Hays County Development Services Department, 2171 Yarrington Road, Suite 100, Kyle, TX 78640.

[FR Doc. 2025–15882 Filed 8–19–25; 8:45 am]
BILLING CODE 9110–12–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2025–0002]

Agency Information Collection Activities: Extension/Renewal of a Currently Approved Information Collection for Cybersecurity and Infrastructure Security Agency (CISA) Visitor Request Form

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

ACTION: 60-Day notice and request for comments; This a renewal of existing 11000–39 Visitor Request Form, 1670–0036 that was previously approved on August 05, 2022, with an expiration date of August 31, 2025.

SUMMARY: The Office of the Chief Security Officer (OCSO) 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.

DATES: Comments are encouraged and will be accepted until October 20, 2025.

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

ADDRESSES: You may submit comments, identified by docket number Docket #CISA–2025–0002, by following the instructions below for submitting comment via the Federal eRulemaking Portal at *http://www.regulations.gov*.

Instructions: All comments received must include the agency name and docket number Docket #CISA–2025–0002. 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: Michael A. Washington, Jr., 703–235–1925, *Michael.Washington@mail.cisa.dhs.gov*.

SUPPLEMENTARY INFORMATION: Public Law 107–296 The Homeland Security Act of 2002, Title II, recognizes the Department of Homeland Security's role in integrating relevant critical infrastructure and cybersecurity information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities while maintaining positive control of sensitive information regarding the national infrastructure. In support of this mission, CISA Office of the Chief Security Officer (OCSO) must maintain a robust visitor screening capability.

CISA OCSO will collect, using an electronic form, information about each potential visitor to CISA facilities and the nature of each visit. CISA OCSO will use collected information to make a risk-based decision to allow visitor access to CISA facilities.

This is an extension of an existing information collection.

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: Cybersecurity and Infrastructure Security Agency (CISA) Visitor Request Form.

OMB Number: 1670–0036.

Frequency: Annually.

Affected Public: Private and Public Sector.

Number of Respondents: 20,000.

Estimated Time per Respondent: 10 minutes.

Total Burden Hours: 3,333 hours.

Total Annualized Respondent Cost: $158,010.66.

Total Annualized Government Cost: $366,514.16.

Robert J. Costello,

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

[FR Doc. 2025–15860 Filed 8–19–25; 8:45 am]
BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Actively Exploited Vulnerability Submission Form

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

ACTION: 30-Day notice and request for comments; new collection request and OMB control number is 1670–NEW.

SUMMARY: The Vulnerability Management (VM) within Cybersecurity

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.