The Deputy Director for Extramural Research, Jon Lorsch, having reviewed and approved this document, authorizes Alycia Booth, who is the Federal Register Liaison, to electronically sign this document for purposes of publication in the **Federal Register**.

Dated: July 6, 2026.

**Alycia Booth,**

*Federal Register Liaison, National Institutes of Health.*

[FR Doc. 2026–16300 Filed 8–10–26; 8:45 am]

**BILLING CODE 4140–01–P**

## DEPARTMENT OF HOMELAND SECURITY

**[Docket No. CISA–2026–0133]**

### Infrastructure Security Division, Cybersecurity and Infrastructure Security Agency, Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Cybersecurity and Infrastructure Security Agency Vulnerability Assessments

**AGENCY:** Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.

**ACTION:** 60-Day notice and request for comments; Cybersecurity and Infrastructure Security Agency VULNERABILITY ASSESSMENTS, 1670–0035.

**SUMMARY:** The Infrastructure Security Division, an office within Cybersecurity and Infrastructure Security Agency submits the following information collection request) to the Office of Management and Budget for review and clearance. The is an extension of a previously cleared information collection request on November 15, 2023, with an expiration date of November 30, 2026. The purpose of this notice is to allow additional 60 days for public comments.

**DATES:** Comments are encouraged and will be accepted until September 10, 2026. Submissions received after the deadline for receiving comments may not be considered.

**ADDRESSES:** You may submit comments, identified by docket number Docket # CISA–2026–0133, 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–2026–0133. 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:** If additional information is required contact: Iesha Alexander, 202–440–0834, *iesha.alexander@cisa.gov.*

**SUPPLEMENTARY INFORMATION:** On April 30, 2024, the White House National Security Council published the National Security Memorandum 22 (NSM–22) on Critical Infrastructure Security and Resilience, which builds on the important work that the Cybersecurity and Infrastructure Security Agency has been undertaking in partnership with America's critical infrastructure communities. Replacing the previous Presidential Policy Directive 21 (PPD–21) on Critical Infrastructure Security and Resilience, is the National Security Memorandum will help ensure U.S. critical infrastructure can provide the nation a strong and innovative economy, protect American families, and enhance our collective resilience to disasters before they happen, strengthening the nation for generations to come. This National Security Memorandum specifically:

- Task the U.S. Department of Homeland Security to coordinate the national effort to enhance the security and resilience of United States critical infrastructure and provide strategic guidance on this national effort, with Cybersecurity and Infrastructure Security Agency acting as the National Coordinator for the Security and Resilience of U.S. Critical Infrastructure. The Secretary of Homeland Security will be required to submit to the President a biennial National Risk Management Plan that summarizes U.S. government efforts to mitigate risk to the nation's critical infrastructure.
- Reaffirms the designation of 16 critical infrastructure sectors and establishes a federal department or agency responsible for managing risk within each of these sectors.
- Elevates the importance of minimum security and resilience requirements within and across critical infrastructure sectors, consistent with the National Cyber Strategy, which recognizes the limits of a voluntary approach to risk management in the current threat environment.

The Cybersecurity and Infrastructure Security Agency Act of 2018 provides the Cybersecurity and Infrastructure Security Agency with a mission, mandate, and responsibility to take various measures and lead various efforts to help secure the nation's critical infrastructure. To support this mission, Cybersecurity and Infrastructure Security Agency's Infrastructure Security Division conducts voluntary on-site security and resiliency assessments for various critical infrastructure entities, which requires Cybersecurity and Infrastructure Security Agency to voluntarily collect certain information about an entity's security posture, for example; the alignment of their security with business objectives, provide a baseline against which improvements can be measured, and by helping demonstrate due diligence to regulators, customers, and stakeholders. These assessments are web-based and are used to collect an organization's basic high-level information and its dependencies. This data is then used to determine a Protective Measures Index and a Resilience Measure Index for the assessed organization. In turn, the Protective Measures Index and the Resilience Measure Index allow the organization to see how it compares to other organizations within the same sector as well as allows them to see how adjusting certain aspects would change their protection and resiliency readiness. This allows the organization to then determine where best to allocate funding and perform other high-level decision-making processes pertaining to the security and resilience of the organization.

The information will be voluntarily provided by the organizations to Cybersecurity and Infrastructure Security Agency Protective Security Advisors and Cybersecurity Security Advisors. The Protective Security Advisors and Cybersecurity Advisors will then visit the site and perform the assessment, as requested. They then return to complete the vulnerability assessment and input the data into the system where the data is then accessible by the system users. Once available, the organization and other relevant system users can then review the data and use it for planning, risk identification, mitigation, and decision making.

All data captured is electronically by the Protective Security Advisors, Cybersecurity Advisors or by the organization as a self-assessment. Participation in the vulnerability assessments is voluntary but full completion of the assessment data collection is required if the organization desires to receive a complete evaluation of their security posture.

After assessments are input into the system, the user is prompted to participate in a feedback questionnaire called the Post Assessment questionnaire. Participation in the Post Assessment questionnaire is voluntary. The Post Assessment Questionnaires are designed to capture feedback about a vulnerability assessment and the system. There are three different questionnaires correlated and prompted after entering a particular assessment into the database. The results are used internally within the U.S. Department of Homeland Security to make programmatic improvements. After assessments are input into the system, the user is prompted to participate in a feedback questionnaire.

The collection of information uses automated electronic vulnerability assessments and questionnaires. The vulnerability assessments and questionnaires are electronic in nature and include questions that measure the security, resiliency and dependencies of an organization. The vulnerability assessments are arranged at the request of an organization and are then scheduled and performed by Protective Security Advisors.

The changes to the collection since the previous OMB approval includes the transition of three cyber-centric questionnaires customer feedback questionnaires (Cybersecurity Infrastructure Survey, Cyber Resilience Review, and External Dependency Management) to a disparate system, and the decommissioning of the Stakeholder Risk Assessment and Mitigation. These actions reflect a strategic consolidation of assessment functions and the migration of questionnaire content and capabilities to an alternative system. Collectively, these modifications have resulted in reduced respondent burden and associated cost estimates, as the retired questionnaires and system components are no longer part of the information collection framework.

The removal of the three questionnaires has decreased the burden estimates by $1,264,787. The annual burden cost for the collection has decreased by $1,267,072, from $1,907,757 to $640,685, due to the removal of the Post Assessment Questionnaires and updated wage rates. The annual government cost for the collection has decreased by $1,478,073, from $2,220,152 to $742,079, due to the removal of the three Post Assessment Questionnaires and updated wage rates. The information collected is also shared with the Federal Emergency Management Agency and is utilized to make determinations for Public Assistance grants based on the information supplied by the respondents.

Cybersecurity and Infrastructure Security Agency is authorized by the Cybersecurity and Infrastructure Security Agency Act of 2018 to collect this information codified under the authorities provided by 6 United States Code, section 652, including subsection (c)(5) (authorizing the Cybersecurity and Infrastructure Security Agency to ''upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies''); and (e)(1)(B) (authorizing the Cybersecurity and Infrastructure Security Agency to ''carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States'').

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, U.S. Department of Homeland Security.

*Title:* Cybersecurity and Infrastructure Security Agency Vulnerability Assessments.

*OMB Number:* 1670–0035.

*Frequency:* Annually.

*Affected Public:* State, Local, Tribal, and Territorial Governments, and Private Sector Individuals.

*Number of Respondents:* 1,100.

*Estimated Time per Respondent:* 7.5 hours and 0.17 hours depending on response element.

*Total Burden Hours:* 7,150.5.

*Total Annual Burden Cost:* $661,475.

*Total Annual Government Burden Cost:* $883,064.

**Winfield P. Werntz,**

*Acting Chief Information Officer, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.*

[FR Doc. 2026–16270 Filed 8–10–26; 8:45 am]

**BILLING CODE 9111–LF–P**

## DEPARTMENT OF THE INTERIOR

### Fish and Wildlife Service

**[Docket No. FWS–HQ–IA–2026–2476; FXIA16710900000–267–FF09A30000]**

## Endangered Species; Issuance of Permits

**AGENCY:** Fish and Wildlife Service, Interior.

**ACTION:** Notice of issuance of permits.

**SUMMARY:** We, the U.S. Fish and Wildlife Service (Service), have issued the following permits to conduct certain activities with endangered species. We issue these permits under the Endangered Species Act (ESA).

**ADDRESSES:** Information about the applications for the permits listed in this notice is available online at *https://www.regulations.gov.* See **SUPPLEMENTARY INFORMATION** for details.

**FOR FURTHER INFORMATION CONTACT:** Timothy MacDonald, by phone at 703–358–2185 or via email at *DMAFR@fws.gov.* Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

**SUPPLEMENTARY INFORMATION:** We, the Service, have issued permits to conduct certain activities with endangered and threatened species in response to permit applications that we received under the authority of section 10(a)(1)(A) of the Endangered Species Act of 1973, as amended (16 U.S.C. 1531 *et seq.*).

After considering the information submitted with each permit application and the public comments received, we issued the requested permits subject to certain conditions set forth in each permit. For each application for an endangered species, pursuant to section 10(d) of the ESA we found that (1) the application was filed in good faith, (2) the granted permit would not operate to the disadvantage of the endangered species, and (3) the granted permit would be consistent with the purposes and policy set forth in section 2 of the ESA.

**Availability of Documents**

The permittees' original permit application materials, along with public comments we received during public comment periods for the applications, are available for review. To locate the application materials and received comments, go to *https://www.regulations.gov* and search for the appropriate permit number (*e.g.,* 12345C) provided in the following table: