[FR Doc. 2024–23124 Filed 10–4–24; 8:45 am]
BILLING CODE 9110–12–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0025]

Agency Information Collection Activities: Incident Reporting Form

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

ACTION: 60-Day notice and request for comments; new Information Collection Request, 1670–NEW.

SUMMARY: The Cybersecurity Division (CSD) within the 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. This is a replacement to an existing collection and is a new collection request. This ICR collects cybersecurity incident reports related to Federal agency information systems, mandatory reports on behalf of certain Federal regulatory agencies, mandatory reports due to contractual requirements, and voluntary reports from members of the public. This ICR, which is authorized by the Federal Information Security Modernization Act of 2014 (FISMA) and the Homeland Security Act, is distinct from incident reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CISA will use a different information collection instrument for CIRCIA incident reports after the effective date of CIRCIA implementing regulations. The questions included in this package for public review represent the universe of all possible questions CISA may use for incident report information collection purposes across multiple use cases; no respondent will be presented all the questions.

DATES: Comments are encouraged and will be accepted until December 6, 2024.

ADDRESSES: You may submit comments, identified by docket number Docket –CISA–2024–0025, 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–2024–0025. 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: Brian DeWyngaert; 202–657–1360; *Brian.dewyngaert@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: CISA serves as ''a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities.'' 6 U.S.C. 659(c)(1).

CISA is responsible for performing, coordinating, and supporting response to information security incidents, which may originate outside the Federal community and affect users within it, or originate within the Federal community and affect users outside of it. CISA uses the information from incident reports to develop timely and actionable information for distribution to Federal departments and agencies; State, local, Tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations. Often, the effective handling of security incidents relies on information sharing among individual users, industry, and the Federal Government, which may be facilitated by and through CISA.

Pursuant to the *Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. 3552 et seq.,* CISA operates the Federal information security incident center for the United States Federal Government. 44 U.S.C. 3556. Federal agencies notify and consult with CISA regarding information security incidents involving Federal information systems. CISA provides Federal agencies with technical assistance and guidance on detecting and handling security incidents, compiles and analyze incident information that threatens information security, informs agencies of current and potential threats and vulnerabilities, and provides intelligence or other information about cyber threats, vulnerabilities, and incidents to agencies. 44 U.S.C. 3556(a). CISA also receives incident reports from non-Federal entities who are reporting to satisfy existing regulatory, statutory, and/or contractual requirements. Finally, CISA receives voluntary incident reports from non-Federal entities.

CISA's website (at *https://www.cisa.gov/*) is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with CISA. Constituents, which may include anyone or any entity in the public, use forms located on the website to complete these activities. Incident reports are primarily submitted using CISA's current Incident Reporting Portal, available at *https://www.cisa.gov/forms/report.* This new collection instrument will replace the current form once the new collection instrument is online and active.

By accepting incident reports and feedback, and interacting among Federal agencies, industry, the research community, State and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public, CISA has provided a way for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government about cybersecurity.

Incident reports are collected through the Incident Reporting Portal, which enables end users to report incidents and indicators as well as submit malware artifacts associated with incidents to CISA. This information is used by CISA to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate. This ICR also requests the user's name, email address, organization, and infrastructure sector. The primary purpose for the collection of this contact and industry information is to allow CISA to contact requestors regarding their report.

In addition to web-based electronic forms, information may be collected through email or telephone. These methods enable individuals, private sector entities, personnel working at other Federal or State agencies, and international entities, including individuals, companies and other nations' governments to submit information.

This collection of information will replace CISA's current Incident Reporting Form. There are significant changes to the current set of questions asked. The questions included in this package for public review represent the universe of all possible questions CISA may use for incident report information collection purposes across the multiple use cases outlined above; no respondent will be presented all the questions. In the Incident Reporting Portal respondents will be directed to answer a subset of the questions based on the characteristics of the reporting entity, the reasons for which they are reporting, and the nature of the incident. The dynamic design of the Incident

Reporting Portal means that the user experience flow from question to question is driven by the individual respondent's responses. No respondent will be prompted to answer all the questions included in this package for review and approval.

This collection of information is distinct from CISA's efforts to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) covered cyber incident and ransom payment reporting requirements. On April 4, 2024, CISA published the CIRCIA Notice of Proposed Rulemaking (NPRM). 89 FR 23644 (Apr. 4, 2024). Among other aspects of the proposed rulemaking, the CIRCIA NPRM described the proposed required content of CIRCIA reports. The public comment for that NPRM closed on July 3, 2024, and CISA is currently reviewing and considering comments as it develops the CIRCIA Final Rule. However, CISA clarifies that reporting under CIRCIA will not go into effect until the effective date of the CIRCIA Final Rule, which is anticipated to be late 2025 or early 2026.

As described above, the purpose of this ICR is to replace CISA's current Incident Reporting Form (approved under OMB control number 1670–037) which is used to collect incident reports under CISA's non-CIRCIA authorities (including FISMA) or other existing regulatory, statutory, and/or contractual requirements that provide for reporting of incidents to CISA. This collection is intended to replace the current Incident Reporting Form, prior to the effective date of the CIRCIA Final Rule, with a revised question set that will enrich the value and analytical capabilities on the data collected under these other incident reporting and information sharing authorities.

Because this effort is distinct from the CIRCIA Final Rule development, comments submitted in response to this **Federal Register** notice will not be considered comments on the CIRCIA NPRM or otherwise considered as part of the development of the CIRCIA Final Rule. Further, because CISA is still actively in the process of considering comments received in response to the CIRCIA NPRM, this ICR should not be viewed as indicating how CISA will resolve such comments as part the Final Rule.

This collection of information will not have a significant economic impact on a substantial number of small entities. Based on an average of 26,000 respondents and the current hourly compensation rates, the burden and cost estimates are as follows: the burden hour estimate for an initial report is 52,000 hours and 146,250 hours for subsequent updates to the initial report. The annual burden cost is $8,870,611. The annual government cost is $4,351,165.

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: Clearance for the Collection of Information through CISA Reporting Form.

OMB Number: 1670–NEW.

Frequency: Annually.

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

Number of Respondents: 26,000.

Estimated Time per Respondent: 3 hours (Initial Report) 7.5 hours (Updated Report).

Total Burden Hours: 198,250.

Total Annualized Respondent Cost: $8,870,611.

Total Annualized Government Cost: $4,351,162.

Robert J. Costello,

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

[FR Doc. 2024–23070 Filed 10–4–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF THE INTERIOR

Office of the Secretary

[XXXD5198NI DS61100000 DNINR0000.000000 DX61104]

Exxon Valdez Oil Spill Public Advisory Committee

AGENCY: Office of the Secretary, Interior.

ACTION: Notice of renewal.

SUMMARY: The U.S. Department of the Interior announces the charter renewal of the *Exxon Valdez* Oil Spill Public Advisory Committee.

FOR FURTHER INFORMATION CONTACT: Grace Cochon, U.S. Department of the Interior, Office of Environmental Policy and Compliance, 1011 E Tudor Road, Anchorage, Alaska 99503, 907–227–3781.

SUPPLEMENTARY INFORMATION: The Court Order establishing the *Exxon Valdez* Oil Spill Trustee Council also required the creation of a public advisory group to advise the Trustee Council. Consequently, the *Exxon Valdez* Oil Spill Public Advisory Committee was established and began functioning in October 1992. The Committee consists of 10 members representing the following principal interests: aquaculture/mariculture, commercial fishing, commercial tourism, conservation/environmental, Native landownership, recreation, sport hunting/fishing, subsistence, science/technology, and public-at-large. In order to ensure that a broad range of public viewpoints continues to be available to the Trustee Council, and in keeping with the settlement agreement, the continuation of the Public Advisory Committee is recommended.

In accordance with the provisions of the Federal Advisory Committee Act, as amended (5 U.S.C. Ch. 10), and in consultation with the General Services Administration, the Secretary of the Interior hereby renews the charter for the *Exxon Valdez* Oil Spill Public Advisory Committee.

Certification Statement: I hereby certify that the renewal of the charter for the *Exxon Valdez* Oil Spill Public Advisory Committee is necessary and in the public interest in connection with the performance of duties mandated by the settlement of *United States* v. *State of Alaska,* No. A91–081 CV, and is in accordance with the Comprehensive Environmental Response, Compensation and Liability Act of 1980, as amended and supplemented.