DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Incident Reporting Form

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

ACTION: 30-day notice and request for comment; new information collection request.

SUMMARY: The Cybersecurity Division (CSD) within the Cybersecurity and Infrastructure Security Agency (CISA) will submit 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 October 7, 2024, for a 60-day public comment period. Three (3) comments were received by CISA. One unrelated public comment was submitted. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments will be accepted until **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

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. All submissions received must include the agency name “CISA” and docket number CISA-2024-0025.

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: Brian DeWyngaert, 202-297-7639, brian.dewyngaert@mail.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).

As such, 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 CISA's 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 proposed collection instrument will replace the current form if it is approved by the Office of Management and Budget.

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, e-mail address, organization, infrastructure sector and sub-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 proposed collection of information will replace CISA's current incident reporting form. The questions included in this proposed new incident reporting form represent the universe of all possible questions that CISA may use for incident report information collection purposes across the multiple use cases outlined above. In no circumstance would a respondent be presented all the questions in this proposed collection. In CISA's Incident Reporting Portal respondents will be directed to answer only an applicable 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 1670-0037) 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. In other words, CIRCIA incident reports will utilize their own set of questions, rather than the question set for this information collection request.

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 of the final rule.

CISA Proposed Revisions to this Collection.

CISA proposes to revise this collection as follows:

- CISA maintains most of the questions from the 60-day notice, however, based on comments received, CISA proposes to streamline and consolidate some of the originally proposed questions to reduce burden for respondents that is derived from the collection originally proposed during the 60-day public comment period. CISA proposes to use a further streamlined minimum collection set and augment this minimum set with questions to address the specific data collection needs for FISMA,

Federal Risk and Authorization Management Program (FEDRAMP), or regulations whose regulators use this information collection request to collect reporting information. The dynamic nature of the information collection request will allow CISA to use combinations of the questions, as appropriate, to address reporting needs based upon the context of the report. Overall, the revised question set streamlines and consolidates previously proposed questions, accordingly CISA does not anticipate in increase in burden for this collection.

Responses to Comments Received During 60-Day Comment Period

CISA received three comments during the 60-day public comment period in response to the information collection request (ICR) published in the ***Federal Register*** on October 7, 2024.[1] 89 FR 81097. The three comments received are summarized below along with CISA's response to those comments.

Comment: One commenter suggested that a common issue among critical water infrastructure operations is a need for education on cyberattacks and resilience strategies based on their vulnerabilities. To address this concern and to spot trends affecting these types of entities, the commenter proposed updating the form to collect information on affected organizations' preparedness for the type of incident reported.

Response: CISA agrees with the commenter's suggestion that the additional data would be a valuable way to gauge readiness across sectors or other groups. Further, CISA agrees that this data will improve CISA's ability to draw clearer conclusions about incident impact trends. Therefore, CISA proposes to add an additional question to the collection to gauge across a spectrum the impacted entity's readiness level to handle and respond to the cyber incident. The new question asks, how prepared the entity was to handle and respond to

[1] The unrelated public comment may be viewed at https://www.regulations.gov/comment/CISA-2024-0025-0005. This comment applies to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) covered cyber incident and ransom payment reporting requirements which is out of scope of this proposed collection.

the incident? Answer choices are [Unprepared, Minimally Prepared, Moderately Prepared, Well Prepared] The below are example text which aims to help entities pick the correct choice.

1. Unprepared:

- No incident response plan: No documented procedures for handling cyberattacks.
- Lack of awareness: Employees are not trained on cybersecurity best practices or how to identify threats.
- Basic or no security measures: Weak passwords, outdated software, no firewall or antivirus protection.
- No backups or disaster recovery plan: Data loss is a significant risk.

2. Minimally Prepared:

- Basic incident response plan: A rudimentary document outlining basic steps to take in case of an incident.
- Some security measures: Antivirus software installed, basic firewall, some password policies in place.
- Occasional security awareness training: Employees receive some training, but it may be infrequent or inadequate.
- Basic backups: Some data is backed up, but the process may be inconsistent or incomplete.

3. Moderately Prepared:

- Documented incident response plan: A comprehensive plan with defined roles, responsibilities, and procedures for various incident types.

- Regular security awareness training: Employees receive regular training on cybersecurity best practices, phishing awareness, and incident reporting.
- Robust security measures: Strong passwords, multi-factor authentication, up-to-date software, firewalls, intrusion detection systems, and regular vulnerability scanning.
- Regular backups and disaster recovery plan: Data is regularly backed up and a plan is in place to restore systems and data in case of a major incident.
- Incident response team: A designated team responsible for handling cyber incidents.

4. Well Prepared:

- Advanced incident response plan: A detailed and regularly tested plan that includes incident simulation exercises and post-incident analysis.
- Continuous security awareness training: Ongoing training and education to keep employees up to date on the latest threats and best practices.
- Advanced security measures: Proactive threat hunting, security information and event management (SIEM) systems, advanced malware protection, and penetration testing.
- Comprehensive backups and disaster recovery plan: Multiple backup locations, automated backups, and a detailed plan for business continuity and disaster recovery.
- Dedicated incident response team with external support: A well-trained internal team with access to external cybersecurity experts for specialized assistance.
- Cyber insurance: Coverage for potential financial losses resulting from cyber incidents.

Further CISA will add these key terms as a hover over / tool tip as they relate to cyber incident preparedness:

- Prevention: Implementing security measures to prevent incidents from occurring in the first place.
- Detection: Identifying and detecting incidents as quickly as possible.
- Response: Taking appropriate actions to contain the incident, minimize damage, and restore systems and data.
- Recovery: Restoring normal operations and implementing measures to prevent future incidents.

By understanding these levels of preparedness, we can assess the entities current state and identify areas for improvement to better protect entities with like preparedness profiles.

Comment: One commenter raised the role of Domain Name System (DNS) security logs, Dynamic Host Configuration Protocol (DHCP) data, and Internet Protocol (IP) address management log data in incident response and reporting. The commenter proposed updating the Data Sharing and Logging Readiness section of the form so that respondents could indicate whether they have current and historical DNS security data, DHCP log data, and IP address management log data to share with CISA.

Response: CISA concurs with this suggestion and proposes to add the recommended language to the Data Sharing and Logging Readiness section of the collection.

Comment: One commenter raised that CISA should reduce the number of requested fields and the amount of detail requested in the proposed collection to reduce burden on reporters. Specifically, the commenter suggested that CISA delete or reshape questions pertaining to: "Violation of Law and Policy" (*i.e.*, whether the incident breaches a law or private industry

or policy standard), "Identify the impacted users" (*i.e.*, the types of users impacted by the incident), and "Instance of Impacted Systems" (*i.e.*, a set of questions asking for details on each impacted system, including system type, location, and services provided).

Response: CISA partially agrees with the commenter's suggestions. As detailed above, CISA is proposing a streamlined and consolidated minimum question set to reduce burden for respondents that is derived from and covers the same scope of questions the collection originally proposed during the 60-day public comment period. CISA also agrees that the content surrounding the "Violation of Law and Policy" was unnecessary and proposed removing it from this collection. CISA agrees in part with the suggestion to reshape or eliminate the detailed system information on impacted systems because it could be overly burdensome, in some cases, as suggested by the commentor. When incidents involving destructive (*e.g.*, ransomware) or denial effects are reported, the impacted entity should not be required to provide the full details for each system, and that like systems should be grouped together. However, if specific details of a system or a group of systems lead and/or contributed to the destructive or denial effects experienced by the impacted entity(ies) then, CISA proposes to collect those system details and any associated vulnerabilities. CISA has updated the proposed collection to reflect this change. Finally, CISA partially agrees with the suggestion to eliminate or reshape the proposed the Impacted User content in the proposed collection. CISA has updated the streamlined question set to query for the number of impacted users and not the user type or impact. However, for entities reporting under FISMA, FEDRAMP, or entities covered by other regulations whose regulators who require it, CISA proposes to ask the question as proposed in the 60-day notice. CISA believes that these types of reporting entities should describe the data impact differences of internal users and external users, if both user types had data impacts during the incident, in the incident description and updated as appropriate in supplemental reports. For FISMA, FEDRAMP, and other regulations, this information is necessary for the Federal Government to determine

the impact and scale of the incident, as well as necessary for the Federal Government to determine the appropriate response.

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 $$4,351,162.

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. 2025-01165 Filed: 1/16/2025 8:45 am; Publication Date: 1/17/2025]