Supporting Statement for Paperwork Reduction Act Submissions

Title:
Clearance for the Collection of Information through

CISA Reporting Form

OMB CONTROL NUMBER:1670-NEW

Supporting Statement A

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

Section 2209 of the Homeland Security Act, as amended, established a national cybersecurity and communications integration center to function 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). The Federal Information Security Modernization Act of 2014 (FISMA) established a federal information security incident center and required the Department to operate it. 44 U.S.C. § 3556(a).

The Cybersecurity and Infrastructure Security Agency (CISA) operates the federal information security incident center. Through this center, FISMA required the Department to provide technical assistance and guidance on detecting and handling security incidents, 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). FISMA and implementing policies also require agencies to report information security incidents, major incidents, and data breaches to the federal information security incident center.
44 U.S.C. § 3556(b) (information security incidents), 44 U.S.C. § 3554(b)(7)(C)(iii)(III) (major incidents); Pub. L. No. 113-283, § 2(d) (2014) (codified at 44 U.S.C. § 3553, note (breaches)).

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. Often, therefore, 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.

This is a replacement to an existing collection and is a new collection request. This information collection request (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 of 2022 (CIRCIA). This collection is intended to replace the current incident reporting form (approved under control number 1670-0037), 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.
CISA will use a different information collection instrument for CIRCIA incident reports after the effective date of CIRCIA implementing regulations. 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.

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. This collection instrument, once approved and implemented for use, will replace a similar collection for incident reporting that is currently part of OMB 1670-0037. 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.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

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 cyber security 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.

This information is collected via an 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. The report also requests the user's name, e-mail address, organization, infrastructure sector, infrastructure sub-sector, and other identifying information for the impacted entity and associated points of contact. The primary purpose for the collection of this information is to allow CISA to contact requestors regarding their report.

This ICR includes questions that allow a reporter to identify the applicable regulatory or contractual incident reporting requirements to which the reporter is subject to and within

prearranged agreements with CISA, CISA intends to route incident reports to these other identified regulators or recipients per those agreements. To the extent that reporting to CISA can satisfy reporting requirements, allowing CISA to share these incident reports may make reporting cyber incidents less burdensome to the public. CISA also receives incident reports from non-federal entities who are reporting to satisfy existing regulatory, statutory, and/or contractual requirements.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

Incident reports are primarily submitted using CISA's Incident Reporting Portal. Alternately, information requested in the incident reporting form may be communicated via emails and voice calls, as a backup procedure. CISA does not anticipate collecting significant amounts of information through voice calls. Additionally, anticipated at launch of this ICR, email submission will be supported pending adherence to the appropriate format and data scheme, to be posted prior to launch (time yet to be determined (TBD)). Finally, the ability for automated incident submission is currently being researched and developed and will become an alternative incident reporting option when this capability becomes available (time yet TBD). At time of launch of this ICR, the web form submission will be considered the primary collection method for voluntary incident reports. 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. The future capability of automated reporting and the current web form submission will be the preferred methods of reporting as the alternative methods are phased out in the future (time yet TBD for the phasing out of the alternative methods).

The questions included represent the universe of all possible questions CISA may use for this information collection request. 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.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

This ICR will replace an existing incident reporting form. It will continue to enable users to submit incident information as new incidents occur and provide updates to the incidents as new information is discovered and as corrective actions are performed to resolve the incident.

A search of reginfo.gov provided a few incident reporting collections; however, none of the other incident reporting collections were related to providing a mechanism for reporting cyber incidents outside of the Federal community.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize.

The collection will not have a significant economic impact on a substantial number of small entities, as indicated in item five of OMB Form 83-I. This is due to the voluntary nature of reporting for industry.

In response to comment received from the 60-day notice, 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, 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 particular 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.

6. Describe the consequence to Federal/DHS program or policy activities if the collection of information is not conducted, or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

This ICR is necessary to the proper performance of agency functions. Without active participation from users, the effectiveness of CISA's services supporting incident reporting will be greatly diminished. The questions included in this collection were developed in response to lessons learned and partner feedback provided to CISA over the lifetime of CISA's incident reporting program. The new questions will enable CISA to conduct better incident report prioritization, adversary campaign tracking, and victim engagement as well as to derive more robust insights regarding the national cyber threat landscape which can deliver more value back to reporters through more insightful reporting and more actionable data sharing. If the collection of information is not conducted, then CISA will not be able to improve our existing program to be mitigate these limitations. FISMA requires agencies to report information security incidents, major incidents, and data breaches to the federal information security incident center within CISA and CISA is consequently authorized to receive them. CISA's legal obligations, particularly with respect to reporting of cybersecurity incidents and analysis of incident data, are dependent upon CISA's ability to collect certain information.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

(a) Requiring respondents to report information to the agency more often than quarterly.
(b) Requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it.
(c) Requiring respondents to submit more than an original and two copies of any document.
(d) Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years.

(e) In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study.
(f) Requiring the use of a statistical data classification that has not been reviewed and approved by OMB.
(g) That includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use.
(h) Requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

(a) CISA must be notified of all computer security incidents involving a Federal Government information system. Incidents are essentially unpredictable events, so CISA has little control over the periodicity of incident reporting. Accordingly, incidents and incident reporting can occur more frequently than quarterly. Many reporters submit voluntary reports, and some of these voluntary reporters elect to submit reports frequently.
(b) By their nature, incident reports will need to be submitted in a timely fashion, as soon as possible to the occurrence. Although voluntary public reporting to CISA is not subject to any response deadlines, thirty days to respond may not meet the applicable requirements for mandatory reporting.
(c) N/A
(d) N/A
(e) N/A
(f) N/A
(g) N/A
(h) Other agencies, including DHS Components such as TSA, will use CISA incident reporting capabilities to collect incident information from their regulated public, pursuant to their own authorities. Although reports from regulated entities may be subject to additional regulatory requirements and disclosure protections, such as the TSA's Sensitive Security Information regime, CISA does not control how these other agencies use the information passed to them. Except for questions to automate the routing of reports, CISA has not added questions to this ICR on behalf of these other agencies.

8. Federal Register Notice:
a. Provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.
b. Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.
c. Describe consultations with representatives of those from whom information is to be obtained or those who must compile records. Consultation should occur at least once every three years, even if

the collection of information activities is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

	Date of Publication	Volume #	Number #	Page #	Comments Addressed
60-Day Federal Register Notice:	10/07/2024	89	194	81097-81098	3
30-Day Federal Register Notice	1/17/2025	90	11	5933-5936	0

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. 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 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 term 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.

CISA received zero comments during the 30-day public comment period in response to the information collection request (ICR) published in the ***Federal Register*** on January 17, 2025. 90 FR 5933.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

There is no offer of monetary or material value for this information.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

For qualifying information voluntarily submitted to the government and validated as Protected Critical Infrastructure Information (PCII)[1], the PCII is protected by the government from public disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws, use in civil litigation and for regulatory purpose. CISA does not expect a large number of reports responding to this ICR to be protected by PCII, historical data suggest CISA received less than 10 reports per year that are categorized as PCII.

For details on the PCII regulations please see (6 C.F.R. part 29). The following CISA webpages provide additional information on the PCII program:

- Program webpage: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program
- Frequently asked questions: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions

For qualifying information submitted to the government as Controlled Unclassified Information (CUI) the agency upholds the protections afforded to this CUI with applicable safeguarding or dissemination controls pursuant to and consistent with law, Federal regulations, and Government-wide policies.

For more information on CUI and the CUI Program, please see Executive Order 13556 and the following webpages:

- https://www.archives.gov/cui
- https://www.archives.gov/cui/registry/category-marking-list

PIA coverage is provided by DHS/ALL/PIA-006 DHS General Contact Lists, which covers the collection of contact information to conduct agency operations and DHS/CISA/PIA-026 National Cybersecurity Protection System (NCPS), which covers the system used to collect cyber threat information.

SORN coverage is provided by DHS/ALL-002 DHS Mailing and Other Lists System, which describes the collection and maintenance of records for the purpose of mailing informational literature or responses to those who request it, and for other purposes for which mailing or contact lists may be created.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This

[1] For more information concerning PCII, please see: PCII Program - Frequently Asked Questions | CISA (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

There are no questions of a sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

a. Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desired. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. Generally, estimates should not include burden hours for customary and usual business practices.
b. If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in Item 13 of OMB Form 83-I.
c. Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection activities should not be included here. Instead, this cost should be included in Item 14.

The Cybersecurity and Infrastructure Security Agency (CISA) estimates that a total of 26,000 respondents will respond to this collection per year for the incident reporting form. For the purpose of estimating the burden of this collection, we assume three scenarios of responses per respondent, one initial reporting response for all reports; one response for an update and final reporting for approximately 50% of the incident reports on average; and two updates and a final report for 25% of the incident reports on average.

Initial Report
To determine how long the form would take to complete, CISA conducted usability testing, which resulted in a range of 45 minutes to 90 minutes to complete the form. For this burden estimate, CISA uses 60 minutes (1 hour) as the time necessary to complete the form. This hour burden is broken down into two 30-minute (0.5 hour) sections, one to enter identifying information about the respondent, and another 30 minutes to enter incident-specific information CISA provides this breakdown to be able to account for time spent gathering and preparing incident-specific information for the form. CISA applies a multiplier of four hours outside the form for every hour spent completing the incident specific data on the form, for a total of 2.5 hours to complete the incident-specific information in the incident reporting form[2]. This multiplier is applied only to the time burden necessary to submit the content specifically required to be included in incident reports, as CISA assumes that the identifying information is readily available and would not require a significant additional time burden to gather.

[2] The 2.5-hour burden for the incident specific information is calculated by adding the 0.5 hours to enter the information and the data gathering and preparing time of 2 hours, which was calculated by multiplying the 0.5 hours in the form by the 4 hour multiplier.

In addition to completing the incident report, reporting entities will need to complete identifying information for the impacted entity and associated points of contact. CISA estimates a burden of 0.5 hours for a reporter to submit this identifying information. This would result in a total time burden of three hours to complete an initial incident report.

Update Reports
To estimate the cost of any necessary updated reports, CISA assumes a time burden of 1.5 hours to complete the report. Reporting entities will submit updated reports if substantial new or different information is available beyond the required timelines for an initial report. Thus, CISA anticipates that the process of completing an update report will generally take more time than needed to complete an initial report.

For the purposes of this analysis, CISA assumes that for every hour spent completing the update report, a reporting entity would spend four hours on preparation, for a total of 7.5 hours per update report. For the purposes of this collection, CISA assumes that 50% of all initial respondents (13,000) will submit one update. CISA also assumes that 25% of all initial respondents (6,500) will submit a second update.

Time and Cost Burdens
These time burdens, as well as the numbers of respondents, are shown in Table 1.

To estimate the cost of this collection, CISA multiplies the estimated annual hour burden by the hourly compensation rate for all occupations within the United States, based on Bureau of Labor Statistics (BLS) data. According to BLS, the mean hourly wage for all occupations is $31.48.[3]

To account for benefits and other compensation, this wage rate was multiplied by a compensation factor of 1.4214, to produce an hourly compensation rate of $44.74.[4] Multiplying the total annual hour burden (198,250) by this hourly compensation rate ($44.74) provides an estimated annual cost of $8,870,611. The cost is displayed in Table 1.

Table 1: Estimated Annualized Burden Hours and Costs

Form Name	Number of Respondents	Number of Responses per Respondent	Average Burden per Response (hours)	Total Annual Burden (hours)	Average Hourly Comp. Rate	Total Annual Respondent Cost
	A	B	C	D = A× B × C	E	F = D × E
Incident Reporting Form – Initial	26,000	1	3.0	52,000	$44.74	$2,326,718
Incident Reporting Form	13,000 (50% of reports)	1	7.5	97,500	$44.74	$4,362,596

[3] BLS. Occupational Employment Statistics. May 2023. All Occupations (00-0000). https://www.bls.gov/oes/2023/may/oes_nat.htm#00-0000
[4] BLS Employer Cost for Employee Compensation March 2023 - Table 1. Employer Costs for Employee Compensation by Ownership. https://www.bls.gov/news.release/archives/ecec_03132024.pdf. Based on the values for civilian workers, the compensation factor of 1.4214 is estimated by dividing total compensation ($43.11) by wages and salaries ($30.33).

– Update						
Incident Reporting Form – 2nd Update	6,500 (25% of reports)	1	7.5	48,750	$44.74	$2,181,298
Total	**45,500**			**198,250**		**$8,870,611**

Note: Numbers may not total due to rounding.

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14.)

The cost estimate should be split into two components: (1) a total capital and start-up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of services component. The estimates should take into account costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.

If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection as appropriate.

Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995, (2) to achieve regulatory compliance with requirements not associated with the information collection, (3) for reasons other than to provide information to keep records for the government, or (4) as part of customary and usual business or private practices.

There are no recordkeeping, capital, start-up, or maintenance costs associated with this information collection.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing and support staff), and any other expense that would have been incurred without this collection of information. You may also aggregate cost estimates for Items 12, 13, and 14 in a single table.

To determine the cost to the federal government for this collection, CISA estimated the time burden required for the government to review the collected information. The total estimated annual time

burden for this collection is 45,500 hours. CISA assumes that the person handling the form will be a GS-13 equivalent employee (Step 1) and have an average hourly wage of $56,52.[5] To account for benefits and other compensation, this wage was multiplied by a compensation factor of 1.6919.[6] This equates to an hourly wage of $95.63, which we will multiply by the total hours of 45,500 to obtain a cost estimate of $4,351,162. Table 2 below shows the cost breakdown.

[5] Office of Personnel Management. Salary Table 2024-DCB. Average hourly wage rate for GS-13, Step 1 for the locality pay area of Washington-Baltimore-Arlington, DC-MD-VA-WV-PA. Pay & Leave : Salaries & Wages - OPM.gov

[6] Congressional Budget Office. Comparing the Compensation of Federal and Private-Sector Employees, 2011 to 2015. April 2017. https://www.cbo.gov/publication/52637. According to Table 4, average total compensation for all levels of education is $64.80. According to Table 2, average wages for all levels of education is $38.30. DHS estimates the compensation factor by dividing total compensation by average wages.

Table 2: Annual Government Cost, by Instrument

Form Name	Number of Responses	Average Burden per Response (hours)	Total Time Burden (hours)	Loaded Hourly Compensation Wage	Annual Burden
	A	**B**	**C = A× B**	**D**	**E = C × D**
Incident Reporting Form - Initial	26,000	1	26,000	$95.63	$2,486,380
Incident Reporting Form - Update	13,000	1	13,000		$1,243,190
Incident Reporting Form – 2nd Update	6,500	1	6,500		$621,592
Total	**45,500**		**45,500**		**$4,351,162**

Note: Numbers may not total due to rounding.

The government costs described in this section are difficult to estimate since nearly all the responses on the form do not generate output in the form of a report but rather as input to much larger systems. As such, the estimated **$4,351,162** government cost is a component of a larger cost associated with operating and maintaining the entire system.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I. Changes in hour burden, i.e., program changes or adjustments made to annual reporting and recordkeeping **hour** and **cost** burden. A program change is the result of deliberate Federal government action. All new collections and any subsequent revisions of existing collections (e.g., the addition or deletion of questions) are recorded as program changes. An adjustment is a change that is not the result of a deliberate Federal government action. These changes that result from new estimates or actions not controllable by the Federal government are recorded as adjustments.

This is a new collection request.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

The results of the information collection will not be published for statistical purposes.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain reasons that display would be inappropriate.

DHS will display the expiration date for OMB approval of this information collection.

18. Explain each exception to the certification statement identified in Item 19 "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

DHS does not request an exception to the certificate of this information collection.