Supporting Statement for Paperwork Reduction Act Submissions

Title:
Clearance for the Collection of Information through

CISA Reporting Forms

OMB Control Number: 1670-0037

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) requires the Department to operate a federal information security incident center. 44 U.S.C. § 3556(a).

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 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), see also 6 U.S.C. §659(c) (providing for cybersecurity services for both Federal Government and non-Federal Government entities). FISMA also requires the Department, operating through CISA, to set reporting requirements for information security incidents, major incidents, and data breaches to the federal information security incident center. 44 U.S.C. § 3556 and § 3553(b)(2)(A) (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)). The Cybersecurity Information Sharing Act of 2015 (CISA 2015) requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with certain federal entities in an automated and real-time manner. 6 U.S.C. § 1504(c).

CISA's critical mission activities include:

- Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.
- Developing 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.
- Responding to incidents and analyzing data about emerging cyber threats.
- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.
- Responding to and analyzing control systems-related incidents.
- Conducting vulnerability, malware, and digital media analysis.
- Providing onsite incident response services.
- Providing situational awareness in the form of actionable intelligence.
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations.
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

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.

Per the Federal Information Security Modernization Act of 2014, CISA operates the Federal information security incident center for the United States federal government. Although each federal agency is required to notify and consult with CISA regarding information security incidents involving federal information systems, people and entities outside the Federal Government also report incident information to CISA. Some outside entities provide cybersecurity incident reports to CISA to meet regulatory requirements imposed by the regulators of the entities.

CISA's website (at US-CERT.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.

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. Some regulated entities provide cybersecurity incident reports to CISA to meet applicable regulatory requirements. Incident reports filed pursuant to regulatory requirements (and/or data from them) are shared with the relevant regulatory agency. The information is collected via the following forms:

1. The web-based Incident Reporting Form, DHS Cyber Threat Indicator and Defensive Measure Submission System and Malware Analysis Submission Form enable end users to report incidents and indicators as well as submit malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

2. The Mail Lists Form enables end users to subscribe to the National Cyber Awareness System's mailing lists, which deliver the content of and links to CISA's information sharing products. The user must provide an e-mail address in order to subscribe or unsubscribe, though both of these actions are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

3. The Cyber Security Evaluation Tool (CSET) Download Form, which requests the name, e-mail address, organization, infrastructure sector, country, and intended use of those seeking to download the CSET. All requested fields are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

In order to be responsive to an ever-changing cybersecurity environment, the forms may change to collect data related to current capabilities or vulnerabilities. Standards, guidelines, and requirements of CISA are perpetually adapting to the volatile cybersecurity environment. CISA must retain the ability to update these forms as required, or CISA will be unable to collect critical incident data in support of our mission. Without the necessary tools and methods to collect this information, CISA will be unable to effectively satisfy mission requirements and support our stakeholders through information collection, analysis, and exchange. The general scope and purpose of the forms will remain the same.

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 form, an interactive-submission interface. Alternately, information may be collected through email or telephone calls; however, the interactive web internet reporting form will be the primary collection method for incident reports. The interactive web interface enables 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 in a streamlined manner.

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.

The forms enable users to submit incident information as new incidents occur, provide feedback as corrective action information is published, and register for new subscriptions or upcoming events. Similar information made already pertains to past incidents, products, and events. New submissions contain unique information.

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.

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.

Allowing constituents and members of the public to submit incident information greatly enhances proper performance of agency functions, in accordance with applicable statutes. Analyzing and providing cybersecurity incident and threat information to both Federal Government and non-Federal Government entities is described in 6 U.S.C. § 659(c). CISA's ability to protect federal agencies and the Nation from cyberattacks depend on gathering cyber incident information. Without active participation from a wide variety of users, the effectiveness of CISA's services will fail. CISA's obligations, particularly with respect to receiving and analyzing reports of cybersecurity incidents, 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) There is no applicable requirement for members of the public that lack a cognizable relationship with the government to report incidents with any particular frequency; however, information security incidents may occur many times a quarter. Receiving reports about each incident furthers CISA's statutory mission. CISA must be notified of all computer security incidents, as defined, involving a Federal Government information system within one hour of being positively identified by the agency's Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department.
(b) N/A
(c) N/A
(d) N/A
(e) N/A
(f) N/A
(g) N/A
(h) N/A

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	September 4,	84	171	46554 –	0

Register Notice:	2019			46556	
30-Day Federal Register Notice	January 6, 2020	85	3	516 - 518	1

On September 4, 2019, CISA published a 60-day notice in the Federal Register at 84 FR 46554. CISA has not received any comments related to the 60-day notice.

On January 6, 2020, CISA published a 30-day notice in the Federal Register at 85 FR 516. CISA has received one comment related to the 30-day notice. The commenter, a CISA grant recipient called the Cybercrime Support Network (CSN), offers "helpful guidance" to CISA. The Commenter asserts that its experience in developing training materials and development of a national-level reporting form has provided it insights to "minimize the burden of the collection of information." The commenter thanks CISA for extending the comment period; describes the importance for "DHS and all Federal, State, Local, Tribal, Territorial and Private Sector Partners work together in a holistic fashion to refine cyber incident reporting and information sharing systems;" asks that CISA continue to directly engage the public and consider how changes to the FIRR may complement other cyber incident reporting efforts; and asks that CISA publicly share "lessons learned from the evolution of your incident reporting forms for critical infrastructure with communities of interest."

CISA thanks the commenter for their input. CISA welcomes the input of civil society groups like CSN; as well as, industry; the research community; State, Local, Tribal and Territorial (SLTT) governments; and other members of the public. The nature of the cybersecurity threat to America is growing, and our nation's cyber adversaries move with speed and stealth. CISA has conferred with CSN about its work, including the SLTT Reporting and Threat Information Sharing Pilot, implemented as part of a cooperative agreement with CISA. To perform its mission, CISA needs to be able to receive and share reports of cybersecurity risks and incidents with federal and non-federal entities.

CISA recognizes that its website (at US-CERT.cisa.gov) is a primary tool used by many constituents, including anyone or any entity in the public, to report incident information, access information sharing products and services, and interact with CISA. Accordingly, CISA is renewing and adjusting the incident reporting form to enhance efforts to gather information about cybersecurity incidents and threats. In addition to moving to an interactive web-based design that adapts question sets based on a respondent's input, the information collection focuses on streamlining the user experience by providing clickable response fields and asking questions that are germane to the type of respondent. The adaptive questions and categories are primarily designed to solicit enhanced reporting data from Federal Government entities. Nevertheless, by accepting incident reports and feedback from both the Federal Government and the general public (including critical infrastructure entities) using a unified reporting form, CISA can gather more data and disseminate reasoned and actionable cyber security information to the public; while simultaneously providing a way for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government about cybersecurity. CISA has no objection to publicly sharing lessons learned from the agency's effort to revise its reporting forms, so long as sharing such information is useful to the public, consistent with the agency's mission, and accords with applicable law and federal policy.

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 cyber threat indicators shared under CISA 2015, Federal entities are required to apply appropriate controls to protect the confidentiality of cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is directly related to a cybersecurity threat or a use authorized under CISA 2015 to the greatest extent practicable. *See* 6 U.S.C. § 1504(b); Department of Homeland Security and Department of Justice, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*, June 15, 2018. CISA 2015 also provides additional protections for cyber threat indicators and defensive measures shared consistent with CISA 2015, including considering the cyber threat indicator or defensive measure the commercial, financial, and proprietary information of the submitting non-Federal entity when so designated by the non-Federal entity and exempting the cyber threat indicator and defensive measure from disclosure under section 552 of title 5, U.S. Code, and any state, tribal, or local provision of law requiring disclosure of information or records. 6 U.S.C. § 1504(d). The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. Additionally, some incident reports are subject to protection as Sensitive Security Information under 49 C.F.R. §1520.1 et seq.

This collection is not privacy sensitive, since there is no Personally Identifiable Information (PII) collected or retrieved. Therefore, this collection is not impacted by the Privacy Act and does not require a Privacy Impact Assessment (PIA) or System of Records Notice (SORN).

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 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 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 the Incident Reporting Form per year (this estimate reflects respondents for only the web-based incident reporting form); 22,000 respondents will respond to the DHS Cyber Threat Indicator and Defensive Measure Submission System per year; 2,725 respondents will respond to the Malware Analysis Submission Form per year; 75,000 respondents will respond to the Mail Lists Form per year; and 13,400 respondents will respond to the CSET Download Form per year. For the purpose of estimating the burden of this collection, we assume one response per respondent.

These time burdens, as well as the numbers of respondents, are shown in Table 1. CISA estimates that the Incident Reporting Form will take 0.33 hours (20 minutes) to complete; the DHS Cyber Threat Indicator and Defensive Measure Submission System Form will take 0.17 hours (10 minutes) to complete; and the Malware Analysis Submission, Mail Lists, and CSET Download forms will each take 0.02 hours (1 minute) to complete.

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 $27.07.[1] To account for benefits and other compensation, this wage rate was multiplied by a compensation factor of 1.4534, to produce an hourly compensation rate of $39.23.[2] Multiplying the total annual hour burden (13,852) by this hourly compensation rate ($39.23) provides an estimated annual cost of $543,401. The cost is displayed in Table 1.

[1] BLS. Occupational Employment Statistics. May 2020. All Occupations (00-0000). https://www.bls.gov/oes/2020/may/oes_nat.htm#00-0000

[2] BLS Employer Cost for Employee Compensation - June2021, released on September 16, 2021 https://www.bls.gov/news.release/pdf/ecec_06172021.pdf. Based on the values for civilian workers, the compensation factor of 1.4492 is estimated by dividing total compensation ($38.91) by wages and salaries ($26.85).

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	26,000	1	0.3333	8,667	$39.34	$339,983
DHS Cyber Threat Indicator and Defensive Measure Submission System	22,000	1	0.1667	3,667		$143,839
Malware Analysis Submission Form	2,725	1	0.0167	45		$1,782
Mail Lists Form	75,000	1	0.0167	1,250		$49,036
CSET Download Form	13,400	1	0.0167	223		$8,761
Total	**139,125**			**13,852**		**$543,401**

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 26,080 hours across all eight instruments. CISA assumes that the person handling the forms will be a GS-13 equivalent employee (Step 1) and have an average hourly wage of $49.85.[3] To account for benefits and other compensation, this wage was multiplied by a compensation factor of 1.4492.[4] This equates to an hourly wage of $72.24, which we multiply by the total hours of 26,108 to obtain a cost estimate of $1,886,112. Table 2 below shows the cost breakdown by instrument.

[3] Office of Personnel Management. Salary Table 2021-DCB. Average hourly wage rate for GS-13, Step 1 for the locality pay area of Washington-Baltimore-Arlington, DC-MD-VA-WV-PA (Annual salary of $103,690 divided by 2,080 hours per year = hourly salary of $49.85. Pay & Leave : Salaries & Wages - OPM.gov

[4] BLS Employer Cost for Employee Compensation - June2021, released on September 16, 2021 https://www.bls.gov/news.release/pdf/ecec_06172021.pdf. Based on the values for civilian workers, the compensation factor of 1.4492 is estimated by dividing total compensation ($38.91) by wages and salaries ($26.85).

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	26,000	1	26,000	$72.24	$1,878,295
DHS Cyber Threat Indicator and Defensive Measure Submission System	22,000	0.0019	42		$3,034
Malware Analysis Submission Form	2,725	0	0		$0
Mail Lists Form	75,000	0.0003	26		$1,878
CSET Download Form	13,400	0.0030	40		$2,904
Total	**139,125**		**26,108**		**$1,886,112**

Note: Numbers may not total due to rounding.

The government costs described in this section are difficult to estimate since nearly all the forms do not generate output in the form of a report but rather as input to much larger systems. As such, the estimated $1,886,112 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 revision to an existing form. The changes to the collection since the previous OMB approval include: updating the name of the Agency from NPPD to CISA, removing the ICSJWG Form, and updating the burden and cost estimates.

Based on an increased number of respondents, the revisions to the form, and the updated hourly compensation rates, the burden and cost estimates have increased. The burden hour estimates increased by 7,713 hours, from 6,139 hours to 13,852 hours. The annual burden cost increased by $329,158, from $214,242 to $543,401. The annual government cost increased by $1,379,156, from $506,956 to $1,886,112.

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.