Supporting Statement for Paperwork Reduction Act Submissions

Title:
Clearance for the Collection of Information through US-CERT.gov

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 227 of the Homeland Security Act, as amended established the national cybersecurity and communications integration center (NCCIC) 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. § 148(c)(1). The Federal Information Security Modernization Act of 2014 (FISMA) establishes a federal information security incident center, and requires the Department to operate it. 44 U.S.C. § 3556(a). Consistent with HSPD-23, the United States Computer Emergency Readiness Team (US-CERT), within the NCCIC, generally functions as the federal information security incident center. HSPD-23, at ¶¶ 15, 30. Through this center, FISMA requires 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 also requires agencies to report information security incidents, major incidents, and data breaches to US-CERT. 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)). The Cybersecurity Information Sharing Act of 2015 (CISA) 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).

United States Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) are two branches of NCCIC.

US-CERT'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.

ICS-CERT's critical mission activities include:

- 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; and
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

US-CERT 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 US-CERT. US-CERT fulfills the role of the Federal information security incident center for the United States federal government as defined in the Federal Information Security Modernization Act of 2014. Each federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems (managed by a federal agency, contractor, or other source) that support the operations and assets of the agency. Additional entities report incident information to US-CERT voluntarily.

The US-CERT website is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with US-CERT and its partners within the NCCIC. 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, US-CERT has provided a way for citizens,

businesses, and other institutions to communicate and coordinate directly with the Federal Government about cyber security. The information is collected via the following forms:

1. The Incident Reporting Form, DHS Cyber Threat Indicator and Defensive Measure Submission System and Malware Analysis Submission Form enable end users to report incidents to US-CERT and submit malware artifacts associated with incidents for analysis. The information is used by DHS to conduct analysis and provide warnings of threats to and vulnerabilities of systems, as well as 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 US-CERT'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.
4. The Industrial Control Systems Joint Working Group (ICSJWG) Form, which requests the name, company, e-mail address, and citizenship of the participants at an upcoming ICSJWG meeting. Contact information must be provided in order to submit either form. However, participation in the ICSJWG is optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

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.

All information is collected through web-based, electronic forms, which 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.

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.

It is necessary to the proper performance of agency functions. Without active participation from users, the effectiveness of US-CERT's services will be greatly diminished. This is particularly the case with reporting. FISMA requires agencies to report information security incidents, major incidents, and data breaches to US-CERT and US-CERT is consequently authorized to receive them. For information security incidents that are deemed major incidents, FISMA assigns additional requirements. Within one hour of receiving a notification of a major or significant cyber incident, the Department is required to notify OMB that a major incident has occurred. OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements* 10 (2016). US-CERT's legal obligations, particularly with respect to reporting cyber security incidents, are dependent upon US-CERT'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) US-CERT must be notified of all computer security incidents involving a Federal Government information system with a confirmed impact to confidentiality, integrity or

availability 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**
60Day Federal Register Notice:	July 18, 2017	82	136	32858 - 32859	0
30-Day Federal Register Notice	November 3, 2017	82	212	51288 – 51289	0

A 60-day Federal Register Notice inviting public comments was published on July 18, 2017, 82 FR 32858. No public comments were received.

A 30-day Federal Register Notice inviting public comments was published on November 3, 2017, 82 FR 51288. No public comments were received.

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 defensive measures and indicators shared under CISA, 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 to the greatest extent practicable. 6 U.S.C. § 1504(b). The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

Regarding the rest of the forms, there are no assurances of confidentiality. The collection is not privacy sensitive. No personally identifiable information is being collected; therefore, neither PIA nor SORN coverage is required.

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.

NPPD estimates that a total of 126,395 respondents will respond to this collection per year. This includes respondents for all six forms discussed in this collection. For the purpose of estimating the burden of this collection, we assume one response per respondent, regardless of the form.

Each form will require a different time burden to complete. These time burdens, as well as the numbers of respondents, are shown in Table 1.

Table 1: Time Burden Associated with Forms

Form Name	No. of Respondents	No. of Responses per Respondent	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)
Incident Reporting Form	22,000	1	0.05	1,100
DHS Cyber Threat Indicator and Defensive Measure Submission System	22,000	1	0.1667	3,667
Malware Analysis Submission Form	2,725	1	0.0167	45
Mail Lists Form	75,000	1	0.0167	1,250
CSET Download Form	4,000	1	0.0167	67
ICSJWG Form	600	1	0.0167	10
	126,325			**6,140**

Note: Numbers may not total due to rounding.

To estimate the cost of this collection, the NPPD multiplies the estimated annual hour burden by the loaded wage 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 $23.86.[1] To account for benefits and other compensation, this wage was multiplied by 1.463, to produce a loaded hourly wage of $34.90.[2] Multiplying the total annual hour burden (6,140) by this loaded hourly wage ($34.90) provides an estimated annual cost of $214,243. The cost is displayed in Table 2.

Table 2: Cost Associated with Forms

Form Name	No. of Respondents	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)	Average Hourly Wage Rate	Total Annual Respondent Cost
	(a)	(b)	(c)=(a)x(b)	(d)	(e)=(c)x(d)
Incident Reporting Form	22,000	0.05	1,100	$34.90	$38,390

[1] https://www.bls.gov/oes/2016/may/oes_nat.htm#00-0000
[2] https://www.bls.gov/news.release/ecec.nr0.htm

DHS Cyber Threat Indicator and Defensive Measure Submission System	22,000	0.1667	3,667		$127,967
Malware Analysis Submission Form	2,725	0.0167	45		$1,585
Mail Lists Form	75,000	0.0167	1,250		$43,625
CSET Download Form	4,000	0.0167	67		$2,327
ICSJWG Form	600	0.0167	10		$349
	126,325		**6,140**		**$214,243**

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, NPPD estimated the time burden required for the government to review the collected information. The total estimated annual time burden for this collection is 8,340 hours across all eight instruments. NPPD assumes that the person handling the forms will be a GS-13 equivalent employee and have a loaded wage of $138,600 (loaded wage equals GS-13 salary with Washington, DC area locality pay[3] multiplied by a load factor of 1.46[4] to account for benefits). This equates to an hourly wage of $66.63, which we multiply by the total hours of 7,568 to obtain a cost estimate of $506,956. Table 3 below shows the cost breakdown by instrument.

Table 3: Annual Government Cost, by Instrument

	Avg. Burden per Response (in hours)	Loaded Hourly Wage (GS-13 equiva-lent)	Annual Burden
	(a)	(b)	(c) = (a) x (b)
Incident Reporting Form	7488	$66.63	$498,960
DHS Cyber Threat Indicator and Defensive Measure Sub-mission System	42	$66.63	$2,799
Malware Analysis Submission Form	0	$66.63	$0
Mail Lists Form	26	$66.63	$1,732
CSET Download Form	12	$66.63	$800
ICSJWG Form	40	$66.63	$2,665
Total	7568		$506,956

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

[3] https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/17Tables/html/DCB.aspx

[4] https://www.bls.gov/news.release/ecec.nr0.htm

such, the estimated $506,956 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 information 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/NPPD/CS&C/US-CERT 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/NPPD/CS&C/US-CERT does not request an exception to the certificate of this information collection.