Supporting Statement for Paperwork Reduction Act Submissions

Title: CISA Vulnerability Assessments

OMB Control Number: 1670-0035

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.

The Presidential Policy Directive-21 (PPD-21) (2013) and the National Infrastructure Protection Plan (NIPP) (2013) highlight the need for a centrally managed repository of infrastructure attributes capable of assessing risks and facilitating data sharing. To support this mission need, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has developed a data collection system that contains several capabilities which support the homeland security mission in the area of critical infrastructure (CI) protection.

Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs) conduct voluntary assessments on CI facilities. These assessments are web-based and are used to collect an organization's basic, high-level information, and its dependencies. This data is then used to determine a Protective Measures Index (PMI) and a Resilience Measures Index (RMI) for the assessed organization. This information allows an organization to see how it compares to other organizations within the same sector as well as allows them to see how adjusting certain aspects would change their score. This allows the organization to then determine where best to allocate funding and perform other high-level decision-making processes pertaining to the security and resiliency of the organization.

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.

The information will be gathered by site visits, arranged between the organization owners and DHS PSAs or CSAs. The PSA or CSA will then visit the site and perform the assessment, as requested. They then return to complete the vulnerability assessment and input the data into the system where the data is then accessible to system users. Once available, the organization and other relevant system users can then review the data and use it for planning, risk identification, mitigation and decision making. All data is captured electronically by the PSA, CSA or by the organization as a self-assessment. Participation in the vulnerability assessments is voluntary, but full completion of the assessment data collection is required for the organization to receive a complete evaluation of their security posture.

Below is a list of identified system users and stakeholders.

1. Critical Infrastructure Community
2. Protective Security Advisors (PSAs)
3. State Fusion Centers
4. The State, Local, Tribal, and Territorial Governing Coordinating Council (SLTTGCC)
5. State representatives for critical infrastructure
6. Facility owner/operators
7. DHS Components and Sub-components to include:
    a. Cybersecurity and Infrastructure Security Agency (CISA)
    b. Federal Protective Service (FPS)
    c. Cybersecurity Division (CSD)
        i. Cyber Security Advisors (CSAs)
    d. Infrastructure Security Division (ISD)
        i. Infrastructure Information Collection Division (IICD)
        ii. Sector Outreach and Programs Division (SOPD)
        iii. Protective Security Coordination Division (PSCD)
        iv. National Infrastructure Coordinating Center (NICC)
    e. Transportation Security Administration (TSA)
    f. Office of Health Affairs (OHA)
    g. Sector-Specific Agencies (SSAs)
8. Critical Infrastructure Sectors:
    a. Chemical Sector
    b. Commercial Facilities Sector
    c. Communications Sector
    d. Critical Manufacturing Sector
    e. Dams Sector
    f. Defense Industrial Base Sector
    g. Emergency Services Sector
    h. Energy Sector
    i. Financial Services Sector
    j. Food and Agriculture Sector
    k. Government Facilities Sector
    l. Healthcare and Public Health Sector
    m. Information Technology Sector
    n. Nuclear Reactors, Materials, and Waste Sector
    o. Transportation Systems Sector
    p. Water and Wastewater Systems Sector
9. Army Corp of Engineers

After assessments are input into the system, the user is prompted to participate in a feedback questionnaire. Every user is prompted to participate in the Post Assessment questionnaire after entering an assessment. Participation in the Post Assessment questionnaire is voluntary. The Post Assessment Questionnaires are designed to capture feedback about a vulnerability assessment and

the system. There are three different questionnaires correlated and prompted after entering a particular assessment into the database. The results are used internally within DHS to make programmatic improvements.

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.

The collection of information uses automated electronic vulnerability assessments and questionnaires. The vulnerability assessments and questionnaires are electronic in nature and include questions that measure the security, resiliency and dependencies of an organization. The vulnerability assessments are arranged at the request of an organization and are then scheduled and performed by a PSA or CSA.

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.

There are no known similar programs or information collections that collect information pertaining to critical infrastructure security and resiliency. A search of reginfo.gov also revealed that this information is not collected or duplicated elsewhere.

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 vulnerability assessments do not impact small business or other small entities.

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.

Without the vulnerability assessments, there would be no way for the CI community to effectively measure its security and resiliency. Without the vulnerability assessments, DHS would lack the abilities below:

- Identify and document critical security and resilience information, including physical security, security force, security management, and business continuity;
- Provide information for protective measures, backup procedures planning, and resource allocation;
- Enhance overall capabilities, methodologies, and resources for identifying and mitigating gaps;
- Facilitate information sharing; and
- Benchmark overall security or resilience and demonstrate how assets and sectors are “buying down” risk

(e.g., lowering risk by investing in measures to enhance the security posture of the organization or asset).

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 vulnerability assessments questionnaire, 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.

There are no identified special circumstances at this time that would affect or vulnerability assessments.

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:	July 10, 2019	84	132	32930 – 32931	0
30-Day Federal Register Notice	November 14, 2019	84	220	61923 – 61924	0

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.

The Protected Critical Infrastructure Information (PCII) Program is a crucial tool in facilitating the Department of Homeland Security's (DHS) analysis of infrastructure vulnerability and related information for planning, preparedness, warnings and other appropriate purposes. The PCII Program, implemented by regulation in 6 C.F.R. part 29, enables DHS to collaborate effectively to protect America's critical infrastructure, eighty-five percent of which is in the private sector's hands. The PCII Program authorizes DHS to accept voluntarily-submitted information relating to critical infrastructure from the public, owners and operators of critical infrastructure, and State, local, and tribal governmental entities, while limiting public disclosure of that sensitive information under the Freedom of Information Act, 5 U.S.C. 552 (FOIA), and other laws, rules, and processes. *See, e.g.*, 6 C.F.R. §§ 29.5, 29.6 and 29.8.

PSAs and CSAs are responsible for entering the assessment data by accessing the system. All vulnerability assessments data are submitted in compliance with the PCII Program. Under the PCII Program, critical infrastructure information that is validated as PCII, including the identity of the submitting person or entity and any person or entity on whose behalf the information is submitted, is confidential and protected from disclosure (except as disclosure of PCII is permitted pursuant to regulation). *See* 6 C.F.R. §§ 29.1, 29.2, and 29.8.

The DHS Privacy Office review finds that this a privacy sensitive collection requiring a Privacy Impact Assessment (PIA). The collection is covered by PIA – DHS/NPPD/PIA-023 Infrastructure Protection Gateway.

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.

The vulnerability assessments and questionnaires do not contain any questions that are sensitive in 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 data collection system was designed and built to fill the lack of a repository for the Nation's CI community. Examples of users of the CI community include Federal, state, and county representatives as well as emergency response personnel, organization owners, and security personnel.

CISA estimates that 2,915[1] will complete the vulnerability assessment per year. Each respondent will spend 7.5[2] hours per response and complete one response annually for a total annual burden of 21,863 hours. CISA uses Bureau of Labor Statistics (BLS) wage data for General and Operations Manager occupations to estimate the cost of this collection. The average wage for managers in General and Operations Managers is $59.56.[3] This wage is multiplied by a compensation factor of 1.4621[4] to account for benefits and non-wage compensation, for an hourly compensation rate of $87.09. Multiplying the hourly compensation rate by the estimated total burden hours of 21,863 provides an estimated annual respondent cost of $1.9 million, as shown in Table 1. CISA also estimates that 266 respondents will complete the post assessment questionnaire, and that each respondent will spend 0.17 hours (10 minutes) to complete the questionnaire for a total time burden of 44 hours. Using the same hourly compensation rate as for the previous instrument, CISA estimates a cost for the post assessment questionnaire of $3,861 (44 hours x $87.09). CISA estimates the total cost for both instruments to be $1.91 million.

[1] Figure based on historical trends of average number of system users and numbers of assessments conducted annually

[2] Figure based on historical trends of the average timeframes to complete assessments

[3] Bureau of Labor Statistics OES data. Average wage for Managers in Occupation Code 11-1021. https://www.bls.gov/oes/2018/may/oes111021.htm

[4] BLS. Employer Costs for Employee Compensation – December 2018. Table 1. Employer Costs per Hour Worked for Employee Compensation and Costs as a Percent of Total Compensation: Civilian Workers, by Major Occupational and Industry Group, December 2018. https://www.bls.gov/news.release/archives/ecec_03192019.pdf. The compensation factor of 1.4621 is estimated by dividing total compensation ($59.86) by wages and salaries ($40.94).

Table 1: Estimated Annualized Burden Hours and Costs

Type of Respondent	Form Name	No. of Respondents	No. of Responses per Respondent	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)	Average Hourly Wage Rate	Total Annual Respondent Cost
	Vulnerability Assessments	2915	1	7.50	21863	$87.09	$1,903,897
	Post Assessment Questionnaires	266	1	0.17	44	$87.09	$3,861
Total		**3,181**			**21,907**		**$1,907,757**

Note: Totals may not sum 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 (2) 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 to respondents 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.

CISA estimates that the federal government will respond to all 2,915 vulnerability assessments and all 266 post assessment questionnaires per year. The government burden to respond to a vulnerability assessment will be 7.5[5] hours for an annual burden of 21,863 hours, and the burden to respond to a post assessment questionnaire will be 0.17 hours (10 minutes), for an annual burden of 44 hours. The total burden to government will be 21,907 hours. To estimate the burden to the federal government, the annual burden hours, the estimated annual time burden is multiplied by the fully loaded hourly wage rate. Using the Office of Personnel Management Salary Table for GS14 step 3 wage rate of $59.90[6] per hour multiplied by a load factor of 1.6919[7], we get a total compensation rate of $101.35. Multiplying the compensation rate by the estimated total burden hours of 21,907 provides an estimated annual government cost of $2.22 million, as shown in Table 2.

Table 2: Estimated Government Burden

Instrument	Number of Reports	Average Burden per Report (hours)	Total Time Burden (hours)	Average Hourly Compensation Rate	Total Labor Cost
Vulnerability Assessments	2915	7.50	21863	$101.35	$2,215,659
Post Assessment Questionnaires	266	0.17	44	$101.35	$4,493
Total	**3,181**		**21,907**		**$2,220,152**

Note: Totals may not sum due to rounding

[5] Figure based on historical timeframes to review assessments

[6] Office of Personnel Management. Salary Table 2019-DCB. Average hourly wage rate for GS-14, Step 3. https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/19Tables/html/DCB_h.aspx

[7] 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.

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.

The changes to the collection since the previous OMB approval include: updating the title of the collection, adding three customer feedback questionnaires, increase in burden estimates and costs.

The title of the collection has been updated to better reflect the nature of the instruments within the collection package.

The three questionnaires were added to the collection to provide user feedback on the content and functionality of the system. The addition of the questionnaires have increased the burden estimates by $3,861.

The annual burden cost for the collection has increased by $121,591, from $1,786,166 to $1,907,757, due to the addition of the Post Assessment Questionnaires and updated wage rates.

The annual government cost for the collection has increased by $509,195, from $1,710,959 to $2,220,152, due to the addition of the Post Assessment Questionnaires and updated wage rates.

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 vulnerability assessments and questionnaires will not be published or used outside of the program.

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 the OMB approval.

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

DHS is not requesting an exception.