

Supporting Statement for Paperwork Reduction Act Submissions

Title:

OMB Control Number: 1670-0029

Chemical-Facility Anti-Terrorism Standards Personnel Surety Program 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 CFATS Program identifies and regulates the security of high-risk chemical facilities using a risk-based approach. The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (also known as the CFATS Act of 2014, Public Law 113-254) and also codified the CFATS program into the Homeland Security Act of 2002. See 6 U.S.C. 621 et seq., as amended by Public Law 116-136, Sec. 16007 (2020). The Department implemented the CFATS Program through rulemaking and issued an Interim Final Rule (IFR) on April 9, 2007 and a final rule on November 20, 2007. See 72 FR 17688 and 72 FR 65396.

High-risk chemical facilities regulated by CISA under the CFATS Program must submit a Site Security Plan that describes how they will meet or exceed 18 risk-based performance standards (RBPS), including RBPS 12 -- Personnel Surety. Under RBPS 12, high-risk chemical facilities regulated under CFATS are required to account for the conduct of certain types of background checks in their Site Security Plans. Specifically, RBPS 12 requires high-risk chemical facilities to:

Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including, (i) Measures designed to verify and validate identity; (ii) Measures designed to check criminal history; (iii) Measures designed to verify and validate legal authorization to work; and (iv) Measures designed to identify people with terrorist ties[.]6 CFR § 27.230(a)(12).

The first three aspects of RBPS 12 (checks for identity, criminal history, and legal authorization to work) are performed by the facility. The fourth aspect (i.e., the check for terrorist ties) was implemented in December 2016 at Tier 1 and Tier 2 facilities.¹ In July of 2019 the Cybersecurity and Infrastructure Security Agency (CISA) implemented the CFATS Personnel Surety Program

¹ The initial notice of implementation was published on December 18, 2015 at 80 FR 79058 and may be viewed at <https://www.federalregister.gov/d/2019-14591>.

for all tiers.² A complete description of the CFATS Personnel Surety Program is provided in the July 2019 notice and additional information can be found on CISA’s website.³

As required by the Notice of Action issued by OMB on May 23, 2019, CISA “phased in gradually” the CFATS Personnel Surety Program.⁴ Since July of 2019, when CISA published the implementation notice for the CFATS Personnel Surety Program announcing full implementation, CISA has selected between 50 to 100 facilities a month to update their SSP to implement security measures designed to ensure that certain individuals with or seeking access to the restricted areas or critical assets at those chemical facilities are screened for terrorist ties.

This information collection (1670-0029) expires on May 31, 2022.

History of the Currently Approved Information Collection

In February 2014, the Department submitted an ICR to OMB to establish a single instrument. The request was approved on August 27, 2015.

In August 2018, the Department submitted an ICR to OMB to revise the Information Collection by expanding the respondents to include all high risk chemical facilities. The request was approved on May 23, 2019.

This ICR requests a revision that will: (a) extend the authorization to use the instrument without change for an additional three years, and (b) updates the burden estimates using a new methodology to estimate burden.

Reasons for Revisions

CISA requests that OMB extend this information collection with the following revisions:

- Minor revision to the instrument that reflects the passage of the Cybersecurity and Infrastructure Security Act of 2018, 6 U.S.C. §§ 651-74, such as updating the Agency name to conform with the Agency’s new designation as CISA. CISA is not proposing a change to the scope of the instrument.
- Decrease the annual number of responses from 203,305 to 149,271 responses which is a decrease of 54,304 responses. The revision is based on historical data and a revision in the methodology about how CISA accounts for new facilities. Notably, the new methodology: (a) remove the costs associated with capital/startup costs because they are incorporated within the estimated number of respondents; (b) increases the annual hires rate from 47.8% to 57.3% for total private industry, as estimated from

² The notice of implementation at all high-risk chemical facilities was published on July 9, 2019 at 84 FR 32768 and may be viewed at <https://www.federalregister.gov/d/2019-14591>.

³ Additional information about the CFATS Personnel Surety Program is available at <https://www.cisa.gov/cfats-resources>.

⁴ The Notice of Action issued by OMB on May 23, 2019 about the CFATS Personnel Surety program may be viewed at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201806-1670-001#.

- the Bureau of Labor Statistics (BLS), and (c) increases the number of annual respondents from 72,607.
- An decrease of 9,005 hours of the annual time burden from 33,884 hours to 24,879 hours when compared to the previously approved annual time burden.
 - A decrease in the annual cost burden of \$2,957,074 from \$5,158,226 to \$2,201,152 which reflects (a) removal of the costs associated with capital/startup costs because they are incorporated within the estimated number of respondents, and (b) an increase of the annual reporting and recordkeeping hour and cost burden from 12,101 hours to 24,879 hours as a result of the revised methodology.
 - An increase in the annual cost from \$1,719,409 to \$2,201,152 because of the increase in annual hours as well as an increase in the respondent wage rate from \$85.82/hour to \$88.48/hour, which is based on updated BLS data.
 - A decrease of the overall total annual operating cost to the Federal Government for this collection from \$1,001,189 to \$495,581 based on the projected costs for the government to vet records and the number of submissions.

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.

In accordance with the Homeland Security Act as amended by the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Pub. L. No. 113-254, the following options are available to enable high-risk chemical facilities to facilitate the vetting of affected individuals for terrorist ties.

Option 1. High-risk chemical facilities may submit certain information about affected individuals, which CISA will use to vet those individuals for terrorist ties. Specifically, the identifying information about affected individuals will be compared against identifying information of known or suspected terrorists contained in the Federal Government's consolidated and integrated terrorist watch list, the Terrorist Screening Database (TSDB), which is maintained by the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) in the Terrorist Screening Center (TSC).⁵

Option 2. High-risk chemical facilities may submit information about affected individuals who already possess certain credentials or documentation that rely on security threat assessments conducted by the Department. This will enable CISA to verify the continuing validity of these credentials.

Option 3. High-risk chemical facilities may comply with RBPS 12(iv) without submitting to CISA information about affected individuals who possess Transportation Worker Identification Credentials (TWICs), if a high-risk chemical facility electronically verifies and validates the affected individual's TWICs through the use of TWIC readers (or other technology that is periodically updated using the Canceled Card List).

⁵ For more information about the TSDB, see DOJ/FBI – 019 Terrorist Screening Records System, last published in full as 77 FR 26580 (May 25, 2017).

Option 4. High-risk chemical facilities may visually verify certain credentials or documents that are issued by a Federal screening program that periodically vets enrolled individuals against the TSDB. CISA continues to believe that visual verification has significant security limitations and, accordingly, encourages high-risk chemical facilities choosing this option to identify in their Site Security Plans the means by which they plan to address these limitations.

In addition to the options described above for satisfying RBPS 12(iv), a high-risk chemical facility is welcome to propose alternative or supplemental options in its SSP that are not described in this document. CISA will assess the adequacy of such alternative or supplemental options on a facility-by-facility basis in the course of evaluating each facility's SSP.

Under Option 3 and Option 4, a high-risk chemical facility would not need to submit information about an affected individual to CISA. These Options are only mentioned in this notice for informational purposes, and there will be no analysis of Option 3 and Option 4 in this information collect request.

This information collection request does not propose changes to who qualifies as an affected individual. There are certain groups of persons that CISA does not consider to be affected individuals, such as (1) Federal officials that gain unescorted access to restricted areas or critical assets as part of their official duties; (2) state and local law enforcement officials that gain unescorted access to restricted areas or critical assets as part of their official duties; and (3) emergency responders at the state or local level that gain unescorted access to restricted areas or critical assets during emergency situations.

Information Collected About Affected Individuals

CISA is not proposing a change to the scope of the instrument in the current IC. The information currently collected which CISA is requesting approval to continue to collect is described below.

Option 1: Collecting Information To Conduct Direct Vetting

If high-risk chemical facilities select Option 1 to satisfy RBPS 12(iv) for an affected individual, the following information about the affected individual would be submitted to CISA:

- For U.S. Persons (U.S. citizens and nationals, as well as U.S. lawful permanent residents):
 - Full Name;
 - Date of Birth; and
 - Citizenship or Gender.
- For Non-U.S. Persons:
 - Full Name;
 - Date of Birth;
 - Citizenship; and
 - Passport information and/or alien registration number.

To reduce the likelihood of false positives in matching against records in the Federal Government’s consolidated and integrated terrorist watch list, high-risk chemical facilities would also be able to submit the following optional information about an affected individual to CISA:

- Aliases;
- Gender (for Non-U.S. Persons);
- Place of Birth; and/or
- Redress Number.⁶

High-risk chemical facilities have the option to create and user defined fields to collect and store additional information to assist with the management of an affected individual’s records. Any information collected in this field will not be used to support vetting activities.

Table 1 summarizes the biographic data that would be submitted to CISA under Option 1.

Table 1. Required and Optional Data for an Affected Individual Under Option 1

Data Elements Submitted to CISA	For A U.S. Person	For A Non-U.S. Person
Full Name	Required	
Date of Birth	Required	
Gender	Must provide Citizenship or Gender	Optional
Citizenship		Required
Passport Information and /or Alien Registration Number	N/A	Required
Aliases	Optional	
Place of Birth	Optional	
Redress number	Optional	
User Defined Field(s)	Optional (Not used for vetting purposes)	

Option 2: Collecting Information To Use Vetting Conducted Under Other DHS Programs

In lieu of submitting information to CISA under Option 1 for vetting of terrorist ties, high-risk chemical facilities also have the option, where appropriate, to submit information to CISA to electronically verify that an affected individual is currently enrolled in another DHS program that vets for terrorist ties.

To verify an affected individual’s enrollment in one of these programs under Option 2, CISA would collect the following information about the affected individual:

- Full Name;
- Date of Birth; and
- Program-specific information or credential information, such as expiration date, unique number, or issuing entity (e.g., state for Commercial Driver’s License [CDL] associated with an Hazardous Materials Endorsement [HME]).

⁶ For more information about Redress Numbers, please go to <http://www.dhs.gov/one-stop-travelers-redress-process#1>.

To reduce the likelihood of false positives, high-risk chemical facilities may also submit the following optional information about affected individuals to CISA:

- Aliases;
- Gender;
- Place of Birth; and/or
- Citizenship.

High-risk chemical facilities have the option to create and user defined fields to collect and store additional information to assist with the management of an affected individual’s records. Any information collected in this field will not be used to support vetting activities.

Table 2 summarizes the biographic data that would be submitted to CISA under Option 2.

Table 2. Required and Optional Data for an Affected Individual Under Option 2

Data Elements Submitted to CISA	
Full Name	Required
Date of Birth	Required
Program-specific information or credential information, such as expiration date, unique number, or issuing entity	Required
Aliases	Optional
Gender	Optional
Place of Birth	Optional
Citizenship	Optional
User Defined Field(s)	Optional (Not used for vetting purposes)

Other Information Collected

CISA may also contact a high-risk chemical facility or its designees to request additional information (e.g., visa information) pertaining to an affected individual in order to clarify suspected data errors or resolve potential matches (e.g., an affected individual has a common name). Such requests will not imply, and should not be construed to indicate, that an affected individual’s information has been confirmed as a match to a record of an individual with terrorist ties.

CISA may also collect information provided by individuals or high-risk chemical facilities in support of any adjudication requests under Subpart C of the CFATS regulation,⁷ or in support of any other redress requests.⁸

⁷ See 6 CFR 27.300–345.

The information that is collected is used by CISA (1) to compare affected individuals information to known and suspected terrorists, or (2) to electronically verify and validate that the affected individual is enrolled in another DHS program that compares an affected individual's information to known and suspected terrorists.

The purpose of the CFATS Personnel Surety Program is to identify individuals with terrorist ties that have or are seeking access to the restricted areas and/or critical assets at the nation's high-risk chemical facilities.

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.

CISA collects information primarily in electronic format through the CSAT system to enhance access controls and reduce the paperwork burden for chemical facilities.

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.

CISA has provided high-risk chemical facilities and affected individuals alternative options to avoid duplicate vetting when an affected individual is enrolled in another DHS program that performs equivalent vetting for terrorist ties. Specifically, available information is considered in the following ways:

- Under Option 2, CISA will not duplicate the vetting of affected individuals against the Terrorist Screening Database under the CFATS Personnel Surety Program if CISA can verify the affected individual's enrollment in another DHS program.
- Under Option 3, high-risk chemical facilities do not need to submit information about affected individuals enrolled in the TWIC Program, if the facility opts to electronically verify and validate TWICs through the use of a TWIC reader.
- Under Option 4, high-risk chemical facilities will not be required to submit information about affected individuals when they choose to utilize Visual Verification of Credentials Conducting Periodic Vetting, in accordance with section 2102(d)(2)(B) of the Homeland Security Act.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-1), describe any methods used to minimize.

⁸ More information about access, correction, and redress requests under the Freedom of Information Act and the Privacy Act can be found in Section 7.0 of the Privacy Impact Assessment for the CFATS Personnel Surety Program, dated March 10, 2020, and available at [DHS/CISA/PIA 018 Chemical Facility Anti-Terrorism Standards Personnel Surety Program | Homeland Security](#).

While no unique methods will be used to minimize the burden to small businesses, small businesses have flexibility in their SSPs or ASPs to choose which security measures they will implement in order to comply with 6 CFR part 27.

CISA also minimizes the data collected under Option 1 and Option 2 to ensure that it is the minimum necessary to conduct terrorist ties vetting/enrollment verification. CISA minimizes the data collected from all entities, including 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.

Reducing the frequency of information collection would prevent CISA from acquiring up-to-date information about who has or is seeking access to restricted areas and critical assets at high-risk chemical facilities. This could prevent an adequate government response in the event that an affected individual with terrorist ties has or seeks to obtain such access. Furthermore, CISA is prohibited by statute from collecting information about an individual more than once from any owner/operator.

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.

CISA needs to know when new affected individuals obtain or request access to restricted areas/critical assets so that the Federal Government can check to see if they are terrorists and, if so, the Federal Government can take appropriate action. It is important for the government to acquire this information on a rolling basis as new individuals gain access, rather than at fixed (quarterly) intervals, because risks of terrorist attacks materialize as soon as terrorists gain access—these risks cannot be effectively addressed at quarterly intervals.

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.

Table 2: Listing of Federal Register Notices

	Date of Publication	Volume #	Number #	Page #	Comments Addressed
60-Day Federal Register Notice:	06/23/21	86	2021-13110	32960	1
30-Day Federal Register Notice	02/11/22	87	2022-02967	8026	

A 60-day public notice for comments was published in the *Federal Register* on June 23, 2021 at 86 FR 32960.⁹ CISA received one non-germane comment.¹⁰

A 30-day public notice for comments was published in the *Federal Register* on February 11, 2022 at 87 FR 8026.¹¹

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

No payment or gift of any kind is provided to any respondents.

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

No assurance of confidentiality is provided to the respondents. However, some information may be protected from disclosure by CISA under the designation CVI. CVI is a Sensitive but Unclassified designation authorized under Pub. Law 107-296 and implemented in 6 CFR 27.400.

⁹ The 60-day notice may be viewed at <https://www.federalregister.gov/d/2021-13110>.

¹⁰ The nongermane comment may be viewed at <https://www.regulations.gov/comment/CISA-2021-0009-0002>.

¹¹ The 30-day notice may be viewed at <https://www.federalregister.gov/d/2022-02967>.

6 U.S.C. 623(d) states that “in any proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this section, and related vulnerability or security information, shall be treated as if the information were classified material.” In addition, 6 CFR § 27.400(h) specifies the circumstances under which access to CVI may be provided by CISA in the context of an administrative enforcement proceeding.

This is a privacy sensitive system. A Privacy Threshold Analysis has been adjudicated by the DHS Privacy Office which resulted in a determination that PIA coverage is provided by DHS/NPPD/PIA-009(a) Chemical Facility Anti-Terrorism Standards August 12, 2016. SORN coverage is provided by DHS/ALL-002-Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659, DHS/ALL-004-General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792.

Notwithstanding the Freedom of Information Act (FOIA) (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws in accordance with 6 U.S.C. 623(c) and 6 CFR § 27.400(g), records containing CVI are not available for public inspection or copying, nor does CISA release such records to persons without a need to know. *See* 6 CFR 27.400(g)(1).

If a record contains both CVI and non-CVI information, the latter information may be disclosed in response to a FOIA request, provided that the record is not otherwise exempt from disclosure under FOIA and that it is practical to redact the protected CVI from the requested record. *See* 6 CFR 27.400(g)(2).

CISA’s primary IT design requirement is ensuring data security. CISA acknowledges that a non-zero risk exists, both to the original transmission and the receiving transmission, when requesting data over the Internet. CISA has weighed the risk to the data collection approach against the risk to collecting the data through paper submissions and concluded that the web-based approach was the best approach given the risk and benefits.

CISA has taken a number of steps to protect both the data that will be collected through the CSAT Program and the process of collection. The security of the data has been the number one priority of the system design. The site that CISA uses to collect submissions is equipped with hardware encryption that requires Transport Layer Security (TLS), as mandated by the latest Federal Information Processing Standard (FIPS). The encryption devices have full Common Criteria Evaluation and Validation Scheme (CCEVS) certifications. CCEVS is the implementation of the partnership between the National Security Agency and the National Institute of Standards (NIST) to certify security hardware and software.

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 standard questions of a sensitive nature. However, CISA may ask questions of a sensitive nature to confirm that an affected individual is or is not a match to a known or suspected terrorist in the Terrorist Screening Database (TSDB).

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.

Since implementing the Personnel Surety Program, CISA has received information about affected individuals from 1,666 facilities, totaling 228,337 respondents, for an average of 137.1 respondents per facility. CISA expects to have fully implemented the CFATS Personnel Surety Program at all existing high-risk chemical facilities by the end of CY21 and prior to the expiration date of this ICR (i.e., May 31, 2022).

To account for new hires and industry turnover, CISA applies the annual hires rate of 57.3% for total private industry, as estimated from the Bureau of Labor Statistics (BLS)¹² to the total number of respondents checked for terrorist ties, resulting in 130,837 annual respondents.¹³

Additionally, CISA estimates the number of annual respondents for facilities determined to be high risk for the first time by multiplying the number of respondents per facility (137.1) by the average number of new facilities per year (134.5) for an average of 18,434 annual respondents per year. Combining the annual respondents based on hires and the annual respondents based on new high risk facilities, CISA estimates 149,271 annual respondents.

CISA estimates that the time per respondent is 10 minutes (0.1667 hours) per affected individual. To estimate the total time burden, CISA multiplies the per submission burden of 0.1667 hours by the total number of annual submissions of 149,271, for a total time burden of 24,879 hours. To estimate the cost, we multiply the estimated hour burden by the fully loaded annual wage of a site security office (SSO). The SSO's average hourly wage rate of \$88.48 was based on an average hourly wage rate of \$60.81¹⁴ with a benefits multiplier of 1.45496.¹⁵ Therefore, the

¹² https://www.bls.gov/news.release/archives/jolts_03112021.pdf. Table 14

¹³ 228,337 respondents x 57.3% = 130,837

Department estimates the annual cost of this information request to be \$2,201,152 (i.e., 24,879 hours multiplied by \$88.48 per hour).

The instrument burden estimates are summarized in the table below:

Table 3: Instrument Burden Estimate

Instrument	# of Respondents	Responses per Respondent	Average Burden per Response (in hours)	Total Annual Burden (in hours)	Total Annual Burden (in dollars)
	(a)	(b)	(c)	(d) = (a) x (b) x (c)	(e) = (d) x \$85.82
Annual Respondents	149,271	1	0.17 (10 minutes)	24,879	\$2,201,152
Total					\$2,201,152

Accordingly, the annual total estimate for reporting, recordkeeping, and cost burden, under this collection, is \$2,201,152.

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

¹⁴ The wage used for an SSO equals that of Managers, All (11-0000), with a load factor of 1.45496 to account for benefits in addition to wages <https://www.bls.gov/oes/2020/may/oes110000.htm>

¹⁵ Load factor based on BLS Employer Cost for Employee Compensation, December 2020 data, released on March 18, 2021. Load factor = Employer cost for employee compensation (\$38.60) / wages and salaries (\$26.53) = 1.45496 <https://www.bls.gov/news.release/pdf/ecec.pdf>

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 capital or startup costs associated with this collection. While previous versions of this collection included initial submissions as startup costs, CISA has remove the costs associated with capital/startup costs because they are incorporated within the estimated number of respondents and is therefore reflected in question 12.

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.

The annualized cost of this collection to the Federal Government is estimated to be \$495,581. The annualized cost of this collection to the Federal Government is estimated based on the government cost of \$3.32 to vet the records for Option 1 or verify the records for Option 2 multiplied by the number of annual submissions (149,271 submissions x \$3.32 = \$495,581).

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.

There are no program changes or adjustments reported items 13 or 14. The revisions to the burden estimates are described in question 1 of this document and again here:

- Minor revision to the instrument that reflects the passage of the Cybersecurity and Infrastructure Security Act of 2018, 6 U.S.C. §§ 651-74, such as updating the Agency name to conform with the Agency's new designation as CISA. CISA is not proposing a change to the scope of the instrument.
- Decrease the annual number of responses from 203,305 to 149,271 responses which is a decrease of 54,304 responses. The revision is based on historical data and a revision in the methodology about how CISA accounts for new facilities. Notably, the new methodology: (a) remove the costs associated with capital/startup costs because they are incorporated within the estimated number of respondents; (b) increases the annual hires rate from 47.8% to 57.3% for total private industry, as estimated from the Bureau of Labor Statistics (BLS), and (c) increases the number of annual respondents from 72,607.

- An decrease of 9,005 hours of the annual time burden from 33,884 hours to 24,879 hours when compared to the previously approved annual time burden.
- A decrease in the annual cost burden of \$2,957,074 from \$5,158,226 to \$2,201,152 which reflects (a) removal of the costs associated with capital/startup costs because they are incorporated within the estimated number of respondents, and (b) an increase of the annual reporting and recordkeeping hour and cost burden from 12,101 hours to 24,879 hours as a result of the revised methodology.
- An increase in the annual cost from \$1,719,409 to \$2,201,152 because of the increase in annual hours as well as an increase in the respondent wage rate from \$85.82/hour to \$88.48/hour, which is based on updated BLS data.
- A decrease of the overall total annual operating cost to the Federal Government for this collection from \$1,001,189 to \$495,581 based on the projected costs for the government to vet records and the number of submissions.

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.

No plans exist for the use of statistical analysis or to publish this information.

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

The expiration date will be displayed in the instruments.

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

No exceptions have been requested.