Supporting Statement for Paperwork Reduction Act Submissions

Title:

OMB Control Number: 1670-0007

Chemical Security Assessment Tool

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.

Congress initially authorized the CFATS Program under Section 550 of the Department of Homeland Security Appropriations Act of 2007, Pub. L. 109-295 (2006). Congress reauthorized the CFATS Program for an additional five years and three months under the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 and the Chemical Facility Anti-Terrorism Standards Program Extension Act.[1]. The CFATS Act of 2014 codified the Department's authority to implement the CFATS program into the *Homeland Security Act of 2002*. See 6 U.S.C. § 621 et seq., as amended by H.R. 251, 116th Cong. (2019) (enacted).

Section 550 of the *Homeland Security Appropriations Act of 2007*, Pub. L. 109-295 (2006) ("Section 550"), provided (and the CFATS Act of 2014 continues to provide) the Cybersecurity and Infrastructure Security Agency (CISA)[2] with the authority to identify and regulate the security of high-risk chemical facilities using a risk-based approach. On April 9, 2007, the Department issued the CFATS Interim Final Rule (IFR), implementing this statutory mandate. See 72 FR 17688.

Section 550 required (and the CFATS Act of 2014 continues to require) that the Department establish risk-based performance standards (RBPS) for high-risk chemical facilities. Through the CFATS regulations, the Department promulgated 18 RBPS. Each covered chemical facility determined by CISA to be high-risk must submit, for CISA approval, a Site Security Plan (SSP) or an Alternative Security Program (ASP), whichever the high-risk chemical facility so chooses, that satisfies each applicable RBPS.

---

[1] The CFATS Act of 2014 codified the CFATS program into the Homeland Security Act of 2002. See 6 U.S.C. 621 et seq.; *see also* The Chemical Facility Anti-Terrorism Standards Program Extension Act. Pub. L. 116-2 (2019).

[2] On November 16, 2018, the President signed the Cybersecurity and Infrastructure Security Agency Act of 2018, which establishes the Cybersecurity and Infrastructure Security Agency. This legislation elevated the mission of the former National Protection and Programs Directorate (NPPD) within the Department and established CISA, with the mission of leading cybersecurity and infrastructure security programs, operations, and associated policy for the Agency, among other functions. The Cybersecurity and Infrastructure Security Agency Act of 2018 was codified at 6 U.S.C. § 652 et seq..

CISA collects the core regulatory data electronically through the Chemical Security Assessment Tool (CSAT).

Reason for Revision
CISA submitted a request for revision to update the burden of the collection. The burden revisions reflect the use of historical data since the information collection was approved in July of 2016 and removal of one-time costs related to a requirement for all chemical facilities to submit a Top-Screen and be evaluated under a revised tiering methodology. CISA submitted the Information Collection Request (ICR) for review to OMB prior to the expiration date.

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.

All information collected supports CISA's effort to reduce the risk of a successful terrorist attack against high-risk chemical facilities. These instruments either directly or indirectly support the affected chemical facilities' requirements to submit data pursuant to 6 CFR Part 27.

Six instruments are in this collection:

(1) Top-Screen,
(2) Security Vulnerability Assessment (SVA) and Alternative Security Program (ASP) Submitted in lieu of an SVA,
(3) Site Security Plan (SSP) and ASP Submitted in lieu of an SSP,
(4) CFATS Help Desk,
(5) User Registration, and
(6) Identification of Facilities and Assets at Risk.

Top-Screen
The purpose of Top-Screen is to obtain information that enables CISA to identify high-risk chemical facilities and obtain an overview of security issues presented by chemical facilities in the nation. CISA electronically collects information via the Top-Screen from chemical facilities that possess screening threshold quantities (STQ) of any chemical of interest (COI) listed in Appendix A of the CFATS regulation. Specifically, 6 CFR § 27.200(b)(2) requires that "A facility must complete and submit a Top-Screen in accordance with the schedule provided in § 27.210, the calculation provisions in § 27.203, and the minimum concentration provisions in § 27.204 if it possesses any of the chemicals listed in Appendix A to this part at or above the STQ for any applicable Security Issue."[3]

The Top-Screen uses the collected data to (1) identify the high-risk chemical facilities covered under the regulation, (2) assign a tier level, and (3) identify security concerns to be addressed in the SVA/ASP and SSP/ASP.

[3] The Department suspended and modified certain submission requirements for chemical facilities of interest and covered chemical facilities in the Federal Register on July 20, 2016 at 81 FR 47001 which may be viewed at https://www.federalregister.gov/d/2016-16776.

6 CFR § 27.200(a) authorizes this instrument to collect "… information from chemical facilities that may reflect potential consequences of or vulnerabilities to a terrorist attack or incident, including questions specifically related to the nature of the business and activities conducted at the facility; information concerning the names, nature, conditions of storage, quantities, volumes, properties, customers, major uses, and other pertinent information about specific chemicals or chemicals meeting a specific criterion; information concerning facilities' security, safety, and emergency response practices, operations, and procedures; information regarding incidents, history, funding, and other matters bearing on the effectiveness of the security, safety and emergency response programs, and other information as necessary." The information is collected electronically by this instrument.

SVA and ASP submitted in lieu of an SVA
The purpose of an SVA/ASP is for high-risk chemical facilities to meet the requirements referenced in 6 CFR § 27.215. Specifically, chemical facilities determined to be high-risk, "must complete a Security Vulnerability Assessment … [which] shall include:

(1) Asset Characterization, which includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection;
(2) Threat Assessment, which includes a description of possible internal threats, external threats, and internally-assisted threats;
(3) Security Vulnerability Analysis, which includes the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards;
(4) Risk Assessment, including a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a success of an attack; and
(5) Countermeasures Analysis, including strategies that reduce the probability of a successful attack or reduce the probable degree of success, strategies that enhance the degree of risk reduction, the reliability and maintainability of the options, the capabilities and effectiveness of mitigation options, and the feasibility of the options."

The information is collected electronically by this instrument.

This instrument also supports CISA's evaluation of submitted SVA/ASPs from high-risk chemical facilities pursuant to 6 CFR § 27.240.

SSP and ASP submitted in lieu of an SSP
The purpose of an SSP/ASP is for high-risk chemical facilities to meet the requirements referenced in 6 CFR §§ 27.225, 27.230, and in 6 CFR §27.235.

The requirements under 6 CFR § 27.225 are as follows

(1) Address each vulnerability identified in the facility's Security Vulnerability Assessment, and identifies and describes the security measures to address each such vulnerability;
(2) Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water-borne explosive devices, ground assault, or other modes or potential modes identified by the Department;
(3) Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard for the appropriate risk-based tier for the facility; and
(4) Specify other information the Assistant Secretary deems necessary regarding chemical facility security.

6 CFR § 27.225(2) requires that facilities "[i]identify and describe how security measures selected by the facility will address the applicable risk-based performance standards." The 19 RBPS are listed in 6 CFR § 27.230. They are as follows:

(1) Restrict Area Perimeter. Secure and monitor the perimeter of the facility;
(2) Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility;
(3) Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,
    i. Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
    ii. Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and discourages abuse through established disciplinary measures.
(4) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:
    i. Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
    ii. Deter attacks through visible, professional, well-maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
    iii. Detect attacks at early stages, through counter surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
    iv. Delay an attack for a sufficient period of time to allow appropriate response through onsite security response, barriers and barricades, hardened targets, and well-coordinated response planning.

(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;
(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;
(7) Sabotage. Deter insider sabotage;
(8) Cyber. Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems;
(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
(10) Monitoring. Maintain effective monitoring, communications and warning systems, including,
    i. Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;
    ii. Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and
    iii. Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions.
(11) Training. Ensure proper security training, exercises, and drills of facility personnel;
(12) Personnel Surety. 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.
(13) Elevated Threats. Escalate the level of protective measures for periods of elevated threat;
(14) Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
(15) Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials;
(16) Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
(17) Officials and Organization. Establish official(s) and an organization responsible for security and for compliance with these standards;
(18) Records. Maintain appropriate records; and
(19) Address any additional performance standards the Assistant Secretary may specify.

CISA continues to collect through a single instrument SSPs and ASPs submitted in lieu of an SSP. Covered chemical facilities that wish to submit an ASP or Expedited Approval Program

(EAP)[4] in lieu of the SSP upload their documentation electronically into the instrument. The information is collected electronically by this instrument.

This instrument also supports CISA's evaluation of submitted SSPs, ASPs, and EAPs submitted in lieu of SSPs pursuant to 6 CFR § 27.245.

CFATS Help Desk
CISA provides technical assistance and consultation to chemical facilities. Inquiries to CISA may be made via a toll-free phone number, web-forms, and email (csat@hq.dhs.gov).

The CFATS Help Desk provides additional customer service functions such as:

(1) The capability for tips about possible security concerns at facilities regulated by CFATS. This allows the general public to report possible security concerns directly to CISA;
(2) Short surveys to solicit feedback and suggestions to improve customer service; and
(3) Verification that an individual is a CVI Authorized User.

The information collected by this instrument takes many forms (e.g., paper, electronic, audio, etc.).

User Registration
The user registration application is a public, web-based tool available through www.dhs.gov/chemicalsecurity for chemical facilities of interest that do not have CSAT user accounts. User Registration is completed and subsequently maintained by the chemical facility Authorizer and/or individuals designated by the Authorizer as having some responsibility for the submission of information collected by CISA through CSAT. The Authorizer role in CSAT is also used by CISA to send official correspondence. Several user roles may be assigned by an Authorizer.

This instrument collects both: (1) basic personally identifiable information (PII) (e.g., full name, contact information, unique identity verification questions) about each individual for their CSAT user account, as well as PII for key security personnel, and (2) facility-related information. Collected facility-related information includes basic demographic information (e.g., location, NAICS, unique identifying names or numbers, relationships to other companies, etc.). The instrument also collects information about "groups" to support the CFATS Personnel Surety Program.

The information is collected electronically by this instrument.

Identification of Facilities and Assets at Risk.
The purpose of Identification of Facilities and Assets at Risk is to collect information from each respondent of an SSP/ASP on their chemical of interest supply and distribution chain or other

[4] The CFATS Expedited Approval Program (EAP) is an option Tier 3 and Tier 4 covered chemical facilities can choose to submit an SSP and certification. SSPs submitted through the EAP for approval to CISA bypass the Authorization and Authorization Inspection steps in the CFATS process and enter directly into the CFATS regulatory cycle. See https://www.dhs.gov/cfats-expedited-approval-program.

information about their business operations. This information will be used by CISA to assist in its efforts to identify either potential chemical facility(s) of interest or potential asset(s) at risk at the covered chemical facility.

Participation in this collection is voluntary and respondents will not be required to provide this information to CISA for purposes of complying with any portion of CFATS.

The information collected by this instrument takes many forms (e.g., paper, electronic, audio, etc.).

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.

This collection continues to use CSAT to reduce the burden on chemical facilities by streamlining the data collection process to meet CFATS regulatory obligations. Collecting the required information primarily through CSAT enhances access controls and reduces the paperwork burden on covered chemical facilities.

Table 1: Medium Information Is Collected In

Name of Instrument	Medium of Collection
Top-Screen	The information is collected electronically by this instrument.
SVA & ASP submitted in lieu of an SVA	The information is collected electronically by this instrument.
SSP & ASP submitted in lieu of an SSP	The information is collected electronically by this instrument.
CFATS Help Desk	The information collected by this instrument takes many forms (e.g., paper, electronic, audio, etc.).
User Registration	The information is collected electronically by this instrument.
Identification of Facilities and Assets at Risk.	The information collected by this instrument takes many forms (e.g., paper, electronic, audio, etc.).

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 maintains the CSAT tool to support the CFATS regulatory program. One of the key features inherent to the CSAT tool is the capability to estimate with a high degree of confidence the health, safety, and security impacts of a terrorist attack. Although State, local, and other Federal regulations relate to chemical safety, those regimes do not collect the core security metrics that enable the identification of high-risk chemical facilities essential to implementing the risk-based security regulation under 6 CFR Part 27.

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.

No unique methods will be used to minimize the burden to small businesses.

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.

6 CFR § 27.210 provides specific submission schedules for chemical facilities data submissions along with revisions to the schedule published at 81 FR 47001 in accordance with § 27.210(a)(2). Additional submission requirements may be found in a high-risk chemical facility SSP/ASP.

6 CFR § 27.200(a) authorizes CISA to "at any time, request information from chemical facilities." This includes both requirements for a facility to (1) resubmit information if a previous submission has been found inadequate, incomplete, contains one or more errors, or otherwise found unacceptable or (2) submit new information necessary for CISA to re-evaluate the facility.

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.

There are no special circumstances with this collection.

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:	February 7, 2019	84	26	2558 – 2564	6
30-Day *Federal Register* Notice	May 7, 2019	84	88	19929 - 19933	0

In response to the 60-day notice for this ICR[5], CISA received one multi-part comment that contained several questions about the instrument "Identification of Facilities and Assets at Risk." As a result of the notice, CISA revised the burden for the instrument. CISA's full response is contained in the 30-day notice.

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.

There is no assurance of confidentiality provided to the respondents, with the exception of whistleblower protections mandated by statute at 6 USC § 625(a)(2).[6]

Some information collected through this collection may be protected from disclosure by the Department under the designation Chemical-terrorism Vulnerability Information (CVI). CVI is a

[5] The 60-day notice for this ICR was published on February 7, 2019 at 84 FR 2558. The notice may be viewed at https://www.federalregister.gov/d/2019-01378.
[6] 6 USC § 625(a)(2) requires CISA to protect the identity of chemical facility employees and contractors who submit reports concerning violation of the CFATS statute and/or regulations. This assurance of confidentiality is provided only through the CFATS Help Desk instrument's tip reporting function. The other information collected through the CFATS Help Desk is not offered any assurance of confidentiality.

Sensitive but Unclassified designation authorized under the CFATS Act of 2014 and implemented in 6 CFR § 27.400.

6 U.S.C. 623(d) states that CVI "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 the Department in the context of an administrative enforcement proceeding.

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 Sec. 550(c) of P.L. 107-296 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 the Department 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 that may not be disclosed under Public Law 107-296 and information that may be disclosed, the latter information may be provided 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).

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.

CISA's primary information technology design requirement was ensuring data security. CISA acknowledges that there is a non-zero risk, 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 CFATS 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.

The instruments described in this collection do not request any information of a personally-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.

Respondents incur reporting and recordkeeping costs due to this information collection. These costs are estimated separately below.

REPORTING BURDEN

To estimate the average annual reporting burden associated with each instrument, CISA multiplies the number of respondents by the annual number of responses per respondent and the estimated time needed to respond. The number of responses per respondent and the time burden estimates vary by instrument and are summarized in Table 2, along with the total annual reporting burden for each instrument.[7]

[7] For detailed information on how CISA estimated the number of respondents, the number of responses per respondent, and the estimated time burden per response for each instrument, please refer to the 30-day notice published at in the *Federal Register* on May 7, 2019 at 84 FR 19929. The notice may be viewed at https://www.federalregister.gov/d/2019-009319.

As shown in Table 2, the estimated annual labor cost associated with reporting is $1.2 million.

Table 2: Estimated Annual Burden Hours and Costs of Reporting by Instrument

Instrument	Number of Respondents A	Number of Responses per Respondent B	Average Burden per Response (hours) C	Total Annual Burden (hours) D = A × B × C	Average Hourly Compensation Rate E	Total Annual Burden Cost F = D × E
CFATS Help Desk	15,000	1	0.17	2,500	$79.69	$199,233
User Registration	1,000	1	2.50	2,500	$79.69	$199,233
Top-Screen	2,332	1	1.09	2,553	$79.69	$203,450
SVA & ASP Submitted in lieu of an SVA	1,683	1	1.24	2,083	$79.69	$166,028
SSP & ASP Submitted in lieu of an SSP	1,683	1	2.72	4,582	$79.69	$365,141
Identification of Facilities & Assets at Risk	3,426	1	0.17	571.00	$79.69	$45,505
Total	**25,124**			**14,789**		**$1,178,590**

Note: Totals may not add due to rounding numbers up or down.

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.

Previously, CISA estimated a one-time cost would be incurred by 3,000 respondents as a result of submitting a Top-Screen to be evaluated under a revised tiering methodology. These one-time costs for respondents have been removed from this information collection.

As described in the 60-day notice, respondents will incur start-up costs and certain respondents would incur operations and maintenance (O&M) costs associated with the recordkeeping of records required under 6 CFR Part 27. CISA estimates that the average annual start-up and O&M costs associated with recordkeeping are $516,825. This includes $80,841 in capital costs and $435,984 in labor associated with recordkeeping.

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 annual cost of this collection is estimated to be $10 million. The annual cost of this collection is based on the Lifecycle Cost Estimate (LCCE) for the CSAT Suite, the information technology investment that supports the collection. The LCCE calculation of the annual cost of maintenance of the CSAT Suite (i.e., the development and testing of minor enhancements and bug fixes) is developed by extrapolation from the actual costs used for CSAT Suite development projects. The LCCE calculation of the annual cost of operation of the CSAT Suite (comprising production hosting services, software licenses, system and database administration, data management, information system security, and help desk services) is based on extrapolation from the actual costs of the current production hosting services.

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.

While CISA made several revisions to the burden estimates since the information collection's last approval in July of 2016, the revisions do not affect the scope of the instruments or collection. CISA also updated the wages and compensation factors used to calculate the labor cost incurred by respondents. The revisions to the collection are outlined in a Supporting Statement Addendum titled "Narrative of Revisions".

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.