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.

On December 18, 2014, the President signed into law the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 ("CFATS Act of 2014") providing long term authorization for the CFATS program. 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*.

Section 550 of Public Law 109-295 previously provided (and the CFATS Act of 2014 continues to provide) the Department 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 and, under CFATS, the Department promulgated 19 RBPS.

CFATS, 6 CFR Part 27, is the Department's regulation governing security at high-risk chemical facilities. CFATS represents a national-level effort to minimize terrorism risk to such facilities. Its design and implementation balance maintaining economic vitality with securing facilities and their surrounding communities. The regulation was designed, in collaboration with the private sector and other stakeholders, to take advantage of protective measures already in place and to allow facilities to employ a wide range of tailored measures to satisfy the regulation's RBPS.

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

History of Collection

In March of 2007, the Department submitted two of the instruments (User Registration and Top-Screen) along with the IFR to OMB, which were authorized at the time the CFATS rule was published in the Federal Register on April 9, 2007.

In May of 2007, the Department submitted an emergency request to OMB for an additional instrument (Chemical-terrorism Vulnerability Information Authorization) along with updates for the two previously submitted instruments. The request was approved on June 6, 2007.

In August of 2007, the Department submitted an emergency request for another two additional instruments (Security Vulnerability Assessment & Site Security Plan) along with updates to the previously submitted instruments. The emergency request was approved on August 23, 2007.

In February of 2008, the Department submitted a request for a three year approval for all the instruments in the collection. The request was approved on May 23, 2008 and the collection was set to expire on May 31, 2001.

In August of 2008, the Department made a minor change to the Chemical-terrorism Vulnerability Information Authorization that did not affect the burden of the instrument. The minor change renamed the instrument to the CVI Training and Authorized User Application and removed the non-disclosure element in the instrument.

In January 2010, the Department submitted a request for revision to modify the burden on many of the instruments based upon historical data since the implementation of the collection. Several of the instruments were refined to reflect the maturing regulatory program. The request was approved on March 23, 2011 and the collection was set to expire on March 31, 2013. The Department submitted the ICR for review by OMB prior to the expiration date.

In March 2013, the Department submitted a request for revision to modify the burden on many of the instruments based upon historical data since the implementation of the collection. Several of the instruments were refined to reflect the maturing regulatory program. The CVI Training and User Authorization instrument was removed from this collection and remains only in the CVI collection (See 1670-0015). The request was approved on September 2014 and the collection was set to expire on April 2016. The Department submitted the ICR for review by OMB prior to the expiration date.

In April 2016, the Department submitted a request for revision to modify the burden on many of the instruments based upon historical data since the implementation of the collection. An instrument was added (Identification of Facilities and Assets At Risk) and several of the instruments were refined to reflect the maturing regulatory program. The Department expects to implement a revised Top Screen, Security Vulnerability Assessment (SVA), and Site Security Plan (SSP) after the CSAT ICR is approved. The Department submitted the ICR for review by OMB prior to the expiration date.

Reason for Revision

This request is submitted to revise a collection which is currently approved but not yet expired. This revision modifies the burden on some of the instruments based upon historical data from January 2012 to December 2014. Some of the instruments are refined to align with section 2102(e)(2) of the Homeland Security Act as amended by the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Pub. L. No. 113-254.[1] Section 2102(e)(2) mandated use of an improved tiering methodology and a maturing regulatory program.

The Identification of Facilities and Assets At Risk instrument has been added to request information from covered chemical facilities about their chemical of interest supply and distribution chain or other information about their business operations to allow the Department to potentially 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 are not required to provide this information to the Department for purposes of complying with any portion of CFATS.

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 the Department's effort to reduce the risk of a successful terrorist attack against high-risk chemical facilities. These collections either directly or indirectly support the affected chemical facilities' requirements to submit data under the CFATS Act of 2014 and CFATS, 6 CFR Part 27.

There are six instruments in this collection:

1. CFATS Helpdesk,
2. CSAT User Registration,
3. CSAT Top-Screen,
4. CSAT Security Vulnerability,
5. CSAT Site Security Plan and Alternative Security Program Submitted in lieu of the CSAT Site Security Plan,
6. Identification of Facilities and Assets At Risk.

CFATS Helpdesk

The Department provides technical assistance and consultation to chemical facilities. Inquiries to the Department may be made via a toll-free phone number, web-forms, and e-mail (csat@hq.dhs.gov).

The CFATS Helpdesk provides additional customer service functions such as:

1. The capability for anonymous tips about possible security concerns at facilities regulated

[1] Section 2 of Pub. L. 113-254 adds a new Title XXI to the Homeland Security Act of 2002. Title XXI contains new sections numbered 2101 through 2109. Citations to the Homeland Security Act of 2002 throughout this document reference those sections of Title XXI. In addition to being found in amended versions of the Homeland Security Act of 2002, those sections of Title XXI can also be found in section 2 of the CFATS Act of 2014, or in 6 USC §§ 621 – 629.

by CFATS. This allows the general public to anonymously report possible security concerns directly to the Department.
2. Short surveys to solicit feedback and suggestions to improve customer service.
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.) as well as content.

CSAT User Registration

CSAT User Registration is completed by the chemical facility Authorizer and/or individuals designated by the Authorizer as having some responsibility for the submission of information collected by the department through CSAT. There are several user roles, which may be assigned by an Authorizer.

This instrument collects both 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 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 CSAT 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. In addition Authorizers or individuals designated by the Authorizer are able to use this tool when logged into the CSAT system to create additional CSAT user accounts and register additional chemical facilities.

The information is collected electronically by this instrument.

CSAT Top-Screen

The purpose of CSAT Top-Screen is to obtain information that enables DHS to identify high-risk chemical facilities and obtain an overview of security issues presented by chemical facilities in the nation. DHS electronically collects information via the Top-Screen from chemical facilities that possess threshold quantities of any chemical of interest 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"

The CSAT Top-Screen uses the collected data to (1) begin the process for identifying the high-risk chemical facilities covered under the regulation, (2) assign the tier level for the facility, and (3) articulate the security concerns to be addressed in the SVA and SSP. The CSAT Top-Screen makes these determinations in a classified database and subsequently sends each covered facility a CVI-protected letter. Information on how the collected data is specifically manipulated in the classified area is available upon request with the proper security clearances and need to know.

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.

The revised CSAT Top-Screen would enable the Department to begin using an improved tiering methodology that incorporates the relevant elements of risk and streamline the entry of information.

This instrument also supports the Department's evaluation of a submitted CSAT Top-Screen pursuant to 6 CFR 27.200(b)(2).

Security Vulnerability Assessment

The purpose of CSAT SVA 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.

The revised CSAT SVA will enable the Department to streamline the entry of information and reduce the amount of time respondents spend in the instrument.

This instrument also supports the Department's evaluation of submitted CSAT SVAs from high-risk chemical facilities pursuant to 6 CFR 27.240.

Site Security Plan & Alternative Security Program submitted in lieu of the Site Security Plan

The purpose of CSAT SSP or ASP in lieu of an SSP is 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 so to allow appropriate response through on-site 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

The Department continues to collect through a single instrument SSPs and ASPs submitted in lieu of an SSP. High-risk chemical facilities that wish to submit an ASP in lieu of the SSP upload their documentation electronically into the instrument. The information is collected electronically by this instrument.

The revised CSAT SSP will enable the Department to streamline the entry of information and reduce the amount of time respondents spend in the instrument.

This instrument also supports the Department's evaluation of submitted CSAT SSPs and ASPs submitted in lieu of CSAT SSPs pursuant to 6 CFR 27.245.

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 a SSP/ASP on their chemical of interest supply and distribution chain or other information about their business operations. This information will be used by the Department 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 will be voluntary and respondents will not be required to provide this information to the Department for purposes of complying with any portion of CFATS.

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 primarily use the Chemical Security Assessment Tool (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 of the high-risk chemical facilities.

Table 1: Medium Information Is Collected In

Name of Instrument	Medium Collection
CFATS Helpdesk	The information collected by this instrument takes many forms (e.g. paper, electronic, audio, etc.) as well as content
CSAT User Registration	The information is collected electronically by this instrument.
CSAT Top-Screen	The information is collected electronically by this instrument.
CSAT Security Vulnerability Assessment	The information is collected electronically by this instrument.
CSAT Site Security Plan & Alternative Security Program submitted in lieu of the Site Security Plan	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.) as well as content

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

The Department developed the CSAT tool for this 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, and thus, the CSAT allows for comparative analysis between chemical facilities. Although there are state, local, and other Federal regulations relating to chemical safety, those regimes do not collect the core security metrics that enable comparative risk analysis across the chemical sector. Comparative risk analysis is 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.

No significant changes were found during a small business analysis when compared to the initial estimates in the regulatory evaluation published in April of 2007.

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 Part 27.210 provides specific submission schedules for chemical facilities data submissions. Additional submission requirements may be found in a high-risk chemical facility Site Security Plan.

6 CFR 27.200(a) authorizes the department 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 the department 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
60Day Federal Register Notice:	November 18, 2015	80	222	72086-72094	12
30-Day Federal Register Notice	April 13, 2016	81	71	21887-21891	7

A 60-day public notice for comments was published in the Federal Register on November 18, 2015, at 80 FR 72086 and specifically solicited comments on four standard questions. The Department received 12 comments submitted by two commenters, which may be found on www.regulations.gov under Docket ID DHS-2015-0058. The two commenters were one private citizen and one industry association. The Department's responses were included in a Paperwork Reduction Act (PRA) 30-day Federal Register notice and are briefly summarized below:

- The Department did not receive any comments suggesting that the proposed collection of information was not necessary for the proper performance of the functions of the agency.
- The Department received four comments that related to the accuracy of the agency's estimate of the burden of the proposed collection of information. Among the comments were comments/suggestions, from the Private Citizen, that (1) individuals or entities couldn't accurately estimate CSAT time and costs; (2) issues associated with facilities potentially required to resubmit Top Screens; and (3) estimations of costs associated with Submitters and Authorizers. The Department responded by noting that actual system statistics were employed in our calculations; only facilities at or above the screening threshold levels would be considered for Top Screens; and the Department employed best estimates costs associated with Submitters and Authorizers, which had been consistently accepted by previous commenters. The Department did not adjust the ICR as a result of these comments.
- The Department received one comment, from the Chlorine Institute, that related to the quality, utility, and clarity of the information to be collected. The comment addressed the use of double negatives in CSAT Tool Suite questioning. The Department responded by stating that the CSAT Tool Suite has been redesigned and reworded confusing questions.
- The Department received two comments, from the Chlorine Institute, that related to minimizing the burden of the collection of information on those who are to respond. The Chlorine Institute noted the use of repetitive questions throughout the CSAT Tool Suite and suggested the use of the RBPS 18 questioning, as a template for the CSAT Tool Suite. The Department responded the CSAT tool suite has been redesigned and, in turn, removed repetitive questions.

- The Department received five comments that were outside the scope of the ICR. Among the comments were suggestions, from the Chlorine Institute, that: (1) Rail cars not be included as a theft issue; (2) the Department employ EPA's RMP submissions in all release scenarios; and (3) the Department consider the use of Pamphlet 74 dispersion estimates in lieu of RMP*COMP. The Department responded by noting that the potential for the theft of rail cars cannot be ruled out; the CFATS program is a security based regulation and not a safety based regulation; and the Department has developed an improved risk methodology that does not use RMP*COMP.

A 30-day public notice for comments was published in the Federal Register on April 13, 2016, at 81 FR 21887. The Department received 9 comments submitted by four commenters, which may be found on www.regulations.gov under Docket ID DHS-2015-0058. The four commenters were all industry associations. The Department responded to each commenter with a letter. The letters may be viewed in the Docket as well under "Supporting Documents." Below is a sample of the comments and suggestions the Department received, which covers the major issues raised by commenters. The Department reviewed and considered all the comments carefully. Based on this review, the Department addressed the comments in the response letters and made a textual clarification to the Top-Screen instrument.

- The Department received three comments related to the proposed collection of information being necessary for the proper performance of the functions of the agency. The comments addressed concerns that without clarifying that only Chemicals of Interest above applicable Screening Threshold Quantities need to be reported, facilities would erroneously report all chemicals regardless of their quantity. The Department responded by adding clarifying text to the Top-Screen Instrument.
- The Department received two comments related to the accuracy of the agency's estimate of the burden of the proposed collection of information. Among the comments were (1) without clarifying that only Chemicals of Interest above applicable Screening Threshold Quantities need to be reported, facilities could not estimate the time costs associated with the submission of the revised Top-Screen, Security Vulnerability Assessment, or Site Security Plan documents, and (2) estimations of costs associated with Submitters and Authorizers. The Department responded by adding clarifying text to the Top-Screen Instrument; and the Department employed the best possible estimations of costs associated with Submitters and Authorizers, which had been consistently accepted by previous commenters.
- The Department did not receive any comments related to the quality, utility, and clarity of the information to be collected, except for the one clarification that it has made to the language regarding chemicals of interest as noted above

- The Department received one comment related to minimizing the burden of the collection of information on those who are to respond. The comment addressed concerns that without clarifying that only Chemicals of Interest above applicable Screening Threshold Quantities need to be reported, facilities would erroneously report all chemicals regardless of their quantity. The Department responded by adding clarifying text to the Top-Screen Instrument.
- The Department received three comments that were outside the scope of the ICR. Among the comments were: (1) facilities were asked to submit an updated Top-Screen because of a change in regulatory compliance standards or enforcement; (2) request for additional background information on the 170-foot radius in determining the distance of concern; and (3) the sharing of distance of concern information as a result of Executive Order 13650. The Department responded by clarifying that only a facility that made an error on their Top-Screen related to their distance of concern, where the error impacted the tiering, were asked to submit an updated Top-Screen; provided additional information on the 170-foot radius; and clarified the Department does not share distance of concern information.

The Department made no changes for the comments received from the 60-day public notice but did make one textual change to the Top-Screen instrument as a result of the comments received from the 30-day public notice. The burden estimates of the ICR have not changed as a result.

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.

The confidentiality of information provided by respondents is covered through several mechanisms.

(1) Chemical-terrorism Vulnerability Information (CVI) is a Sensitive But Unclassified designation authorized under P.L. 109-295 and implemented in 6 CFR 27.400.

(2) CSAT (including CVI Authorized User Training) and CHEMSEC user registration information is covered by DHS/ALL-004 - General Information Technology Access Account Records System (GI-TAARS) System of Records Notice (November 27, 2012, 77 FR 70792).[2]

(3) The CFATS Help Desk and Tip Line information is maintained under the DHS/ALL-002 –

[2] http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm

Department of Homeland Security (DHS) Mailing and Other Lists System of Records (November 25, 2008, 73 FR 71659)[3].

(4) CSAT is covered by the DHS Privacy Impact Assessment (PIA), DHS/NPPD/PIA-009 – Chemical Facility Anti-Terrorism Standards (CFATS) (July 26,2012)[4]

DHS's primary IT design requirement was ensuring data security. DHS acknowledges that there is a non-zero risk, both to the original transmission and the receiving transmission, when requesting data over the Internet. DHS 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.

DHS 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 the Department 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.

[3] http://edocket.access.gpo.gov/2008/E8-28053.htm

[4] https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-cfats.pdf

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 annual total estimate for reporting, recordkeeping and cost burden under this collection is $17,287,100. The Site Security Officers average hourly wage rate of $67.72 was based on an average hourly wage rate of $47.21 with a benefits multiplier of 1.43. The $47.21 rate was based on 2014 dollars using the Consumer Price Index (CPI). U.S. Department of Labor, Bureau of Labor Statistics; ‘‘Table 24. Historical Consumer Price Index for All Urban Consumers (CPI–U): U. S. city average, all;’’ Annual Average; July 2015. Available at: http://www.bls.gov/cpi/tables.htm, last accessed on September 9, 2015. Individual burden estimates vary by instrument and are summarized in the table below:

Table A.12: Estimated Annualized Burden Hours and Costs

Table 2: Instrument Burden Estimate

Instrument	# of Respondents	Responses per Respondent	Total Responses	Average Burden per Response (in hours)	Total Annual Burden (in hours)	Total Recordkeeping Burden (in dollars)	Total Annual Burden Cost (in dollars
Helpdesk	15,000	1	15,000	0.17	2550		172,700
User Registration	1,000	1.00	1,000	2.00	2,000		419,000
TS	1,000	1.50	1,500	6.00	9000		15,623,400
SVA	211	1.50	316.5	2.65	838.725		58,600
SSP/ASP	211	2.00	422	18.75	7912.50	438,800	976,400
Identification of Facilities & Assets At Risks	211	1	211	0.17	35.87		37,000
Totals	17,633		18,449.5		22337.095	438,800	17,287,100

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.

The revised CSAT User Management will enable Authorizers and/or individuals designated by the Authorizer to easily add additional facilities and/or additional CSAT user accounts under the Authorizers CSAT structure. The Department expects that there will be a one-time burden for all existing CSAT Users when the CSAT User Management application is updated. The Department expects the one-time burden to be 0.17 hours (10 minutes) per CSAT user. As of September 2015, there were 24,630 active CSAT accounts, therefore the Department estimates that there will be a capital/startup cost of $283,550.4120 [24,630 Active CSAT users x 0.17 hours x $67.72 (average hourly rate for Site Security Officers)]. The rounded estimate is $283,600.

The revised Top-Screen will enable the Department to begin using an improved tiering methodology that incorporates the relevant elements of risk, which is mandated by Section 2102(e)(2) of the Homeland Security Act of 2002, as amended. The Department may request chemical facilities of interest that have chemical holdings at or above the screening threshold quantities on Appendix A of CFATS to complete the Top-Screen, even if the facility has previously completed a Top-Screen and been determined not to be high-risk under the previous tiering methodology. Between the effective date of CFATS in June of 2007 and December 2014 the Department has received Top-Screens from approximately 36,930 unique facilities. Therefore the Department estimates that there will be a one-time capital/startup cost of $15,005,397.60 [36,930 facilities x 6 hours x $67.72 (average hourly wage rate for Site Security Officers)]. The rounded estimate is $15,005,400.

There are no other annualized capital or start-up costs incurred by chemical facilities of interest or high-risk chemical facilities for this information collection. It is assumed that all chemical facilities of interest and high-risk chemical facilities have the necessary computer hardware and internet connection.

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 $12M. The annual cost of this collection is based on the Lifecycle Cost Estimate (LCCE) for the CSAT Suite, the IT investment that supports the collection. The LCCE calculation of the annual cost of maintenance of the CSAT Suite (development and testing of minor enhancements and bug fixes) is developed by extrapolation from the actual costs for the Agile team structure 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.

Adjustment Change Decrease in the average annual burden as a result of a change in the agency estimates after a review of the historical data collected from January 2012 to December 2014. Program Change Increase in the startup cost. Revised CSAT User Management will enable Authorizers and/or individuals designated by the Authorizer to easily add additional facilities and/or additional CSAT user accounts under the Authorizers CSAT structure. The Department expects that there will be a one-time burden for all existing CSAT Users when the CSAT User Management application is updated. Section 2102(e)(2) of the Homeland Security Act of 2002, as amended, mandates the use of an improved tiering methodology that incorporates the relevant elements of risk. As a result of the development of the new tiering methodology a revised Top Screen must be incorporated. The Department will be requesting chemical facilities that have chemical holdings at or above the screening threshold quantities on Appendix A of CFATS to complete the Top-Screen, even if the facility has previously completed a Top-Screen and been determined not to be high-risk.

Program Change Decrease in the average annual burden for the revised SVA. The revised SVA will:

1. Have duplicative questions removed that exist in the SSP/ASP. Specifically, the Department no longer includes questions related to security equipment, utility systems and infrastructure support, inventory control measures, personnel access control, shipping and

receiving measures, post release measures and equipment, leak detection systems, vapor suppression systems, offsite notification systems, community outreach, cyber control systems, and cyber business systems. In addition, the SVA no longer requires facilities to create individual assets for each tiered COI, but instead allows them to identify locations/areas for their assets which significantly reduces the total number of assets and associated questions that are required to be answered per asset.

2. A few questions will be moved to the Top-Screen to support the improved tiering methodology. These questions include COI storage type, COI physical state, COI temperature, COI pressure, COI concentration, secondary containment, and COI transportation packaging.
3. The attack scenarios and related questions will also be removed. The Department no longer requires facilities to address the eight attack scenarios for each asset identified. Previously this required the facility to answer approximately 240 associated questions for each asset that was identified. In the revised SVA, asset identification requires only four questions, a decrease from 240 to four questions per asset.

Items 1 and 2 above resulted in a decrease in the number of vulnerability questions in the SVA from approximately 600 to 10.

Program Change Decrease in the average annual burden for the revised SSP/ASP. The revised SSP/ASP will

1. Utilize the asset identification from the SVA. Previously, facilities were required to identify assets in both the SVA and SSP. This will remove the asset identification from the SSP.
2. Reorganize the SSP/ASP questions in a streamlined process based upon the Department's experience with respondents over the past several years. This reorganization of SSP/ASP questions allowed the Department to remove repetitive and unnecessary questions, which resulted in removing approximately 1000 questions from the SSP. The previous tool contained approximately 1400 questions plus additional questions based on the number of assets identified. The new tool contains approximately 400 questions and has embedded the asset questions such that repetitive answers are unnecessary.

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.