Supporting Statement for PRA Submission
Chemical Security Assessment Tool
OMB Control Number 1670-0007

A. JUSTIFICATION

1) Circumstances that make the collection of information necessary

Section 550 of P.L. 109-295 provides the Department of Homeland Security with the authority to regulate the security of high-risk chemical facilities. On April 9, 2007, the Department issued an Interim Final Rule (IFR), implementing this statutory mandate at 72 FR 17688. Section 550 requires a risk-based approach to security.

The Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, are the Department's regulations under Section 550 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 regulations were 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 regulations' Risk-Based Performance Standards (RBPS).
CFATS also establishes, in 6 CFR § 27.400, the requirements that covered persons must follow to safeguard certain documents and other information developed under the regulations. This information is identified as "Chemical-terrorism Vulnerability Information" (CVI) and by law receives protection from public disclosure and misuse.

The Department collects the primary 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.

In August of 2008, the Department approved 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. This collection expired on May 31, 2011.

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.

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 2009 to December 2011. Some of the instruments are refined and updated to reflect the maturing regulatory program. The CVI Training and User Authorization instrument has been removed from this collection and will remain only in the CVI collection (See 1670-0015). Recordkeeping costs have been added in the SSP instrument.

2) By whom, how, and for what purpose the information is to be used

All information collected supports the Department's effort to reduce the risk of a successful terrorist attack against chemical facilities. These collections either directly or indirectly support the affected chemical facilities requirements to submit data under Section 550 of P.L. 109-295 and CFATS.

There are five instruments in this collection:

1. CFATS Helpdesk,

2. CSAT User Registration,
3. CSAT Top-Screen,
4. CSAT Security Vulnerability Assessment and Alternative Security Program Submitted in lieu of the CSAT Security Vulnerability Assessment,
5. CSAT Site Security Plan and Alternative Security Program Submitted in lieu of the CSAT Site Security Plan, and

CFATS Helpdesk

Pursuant to 6 CFR 27.210(b), the Department must provide technical assistance and consultation. This instrument collects personally identifiable information and general questions associated with the use of the CSAT computer applications to chemical facilities as well as to the general public, 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 by CFATS. This will allow 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 individuals at a chemical facility identified by the high-risk chemical facility 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 who must be an officer of the corporation or other person designated by an officer of the corporation.

This instrument collects basic personally identifiable information (e.g. full name, contact information, unique identity verification questions) about each individual. It also collects basic demographic information (e.g. location, NAICS, unique identifying names or numbers, relationships to other companies, etc…) about the facility to which the individual may be assigned to provide information about.

The CSAT Registration application is a public, web-based tool available through www.dhs.gov/chemicalsecurity. With a user account, an individual can access the CSAT system.

Upon completion of the Registration form, CSAT generates an Acrobat PDF copy of the registration which the individual prints, signs, and submits to DHS. Once registered, individuals may update their personal information, update information about their facility, and transfer their responsibilities to and from other users with access to CSAT.

The information is collected electronically by this instrument.

CSAT Top-Screen

The primary purpose of CSAT Top-Screen is to identify high-risk chemical facilities and obtain an overview of security issues presented by the nation's chemical facilities. To identify covered facilities, DHS electronically collects information (via the Top-Screen) from a much larger pool of facilities. Specifically, 6 CFR 27.200(b) requires that "A facility must complete and submit a Top-Screen in accordance with the schedule provided in § 27.210 if it possesses any of the chemicals listed in Appendix A to this part at the corresponding Screening Threshold Quantities."

Specifically, 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 preliminary 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 27.210(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 primarily collected electronically by this instrument.

In addition, this instrument collects information to support the management and evaluation of a submitted Top-Screen.

Security Vulnerability Assessment & Alternative Security Program submitted in lieu of the Security Vulnerability Assessment

As part of 6 CFR Part 27.215(a) DHS is required to collect information necessary to determine if "a chemical facility is high-risk".

The SVA collection is taken from facilities completing DHS Form 9015 or by the facility providing their own documentation via an ASP. The ASP can be provided by the facility in a wide variety of forms and formats at the discretion of the facility. DHS is precluded by 6 CFR 27.235(a) (1) from requiring a covered facility preliminarily determined as Tier 4 to submit an SVA. However, all covered facilities preliminarily determined to be Tier 1, Tier 2, and Tier 3 are required to submit an SVA in accordance with 6 CFR 27.235(a)(2). DHS has developed the SVA as part of the Chemical Security Assessment Tool (CSAT) and the data collected will be entered into that system. Covered facilities that wish to submit an ASP in lieu of the SVA will upload their documentation electronically into the CSAT SVA application.

The information collection requirement for the SVA referenced in 6 CFR 27.215 and the ASP referenced in 6 CFR 27.235 are identical because both are compared against a common criteria in 6 CFR 27.240. Specifically, in the 6 CFR 27.235, the ASP section of the regulation states, "The Department will provide … approval or disapproval, in whole or in part, of an ASP, using the procedure specified in [6 CFR] 27.240 if the ASP is intended to take the place of a Security Vulnerability Assessment." 6 CFR 27.240(a) requires that ASPs be evaluated against 6 CFR 27.215, which lists the criteria an SVA must contain. Specifically, "the facility 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 Department continues to collect through a single instrument SVAs and ASPs submitted in lieu of an SVA. The information is primarily collected electronically by this instrument.

In addition, this instrument collects information to support the management and evaluation of a submitted Security Vulnerability Assessment & Alternative Security Program submitted in lieu of the Security Vulnerability Assessment.

Site Security Plan (SSP) & Alternative Security Program submitted in lieu of the Site Security Plan

In 6 CFR Part 27.225(a) the Department is required to collect information necessary to determine that specific security measures meet the following standards:

(1) Address each vulnerability identified in the facility's Security Vulnerability Assessment, that will identify and describe 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.

The Site Security Plan (SSP) will be a DHS-provided standardized form. The ASP is not a DHS standardized form and may be provided to DHS in a wide variety or forms and formats. DHS is precluded from requiring a covered facility to submit a SSP in a mandatory form or format, instead, 6 CFR 27.235(a) allows all covered facilities to submit an ASP in lieu of a SSP. DHS will, however, develop the SSP as

an application in the Chemical Assessment Tool for the benefit of the covered facilities. Covered facilities that wish to submit an ASP in lieu of an SSP will upload the ASP files electronically into CSAT SSP application.

The information collection requirement for the SSP referenced in 6 CFR 27.230 and the ASP referenced in 6 CFR 27.235 are identical because both are compared against a common criteria in 6 CFR 27.245.

Specifically, in the 6 CFR 27.235, the ASP section of the regulation states, "The Department will provide … approval or disapproval, in whole or in part, of an ASP, using the procedure specified in [6 CFR] 27.245 if the ASP is intended to take the place of a Site Security Plan." 6 CFR 27.245 is the Review and Approval of Site Security Plans.

6 CFR 27.245(a) (1) states, "The Department will review and approve or disapprove all Site Security Plans that satisfy the requirements of Sec. 27.225, including Alternative Security Programs submitted pursuant to Sec. 27.235"

6 CFR 27.225(a) requirements are

(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(b) requires that facilities "[i]identify and describe how security measures selected by the facility will address the [19] applicable risk-based performance standards [RBPS]." 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. The information is primarily collected electronically by this instrument.

In addition, this instrument collects information to support the management and evaluation of a submitted SSP/ASP.

3) *Consideration of the use of improved information technology*

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. The facilities may choose to obtain and submit signatures collected for CSAT users by using E-Signatures. 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 primarily collected electronically by this instrument.
Security Vulnerability Assessment & Alternative Security Program submitted in lieu of the Security Vulnerability Assessment	The information is primarily collected electronically by this instrument.
Site Security Plan (SSP) & Alternative Security Program submitted in lieu of the Site Security Plan	The information is primarily collected electronically by this instrument.

4) *Efforts to identify duplication*

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 and safety impacts of a terrorist attack, and thus, the CSAT allows for comparative analysis between chemical facilities. Although there are state, local, and other Federal security regulations relating to chemical security, those regimes do not collect the core metrics that enable comparative risk analysis across the chemical sector. Comparative risk analysis is essential to implementing the risk based regulation required by P.L. 109-295.

5) *Methods to minimize the burden to small businesses if involved*

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) *Consequences to the Federal program if collection were conducted less frequently*

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 will include 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.

CSAT users may call the CFATS Help Desk with questions regarding the CSAT Personnel Surety application. Information about how and when to contact the CFATS Help Desk can be found at http://www.dhs.gov/chemical-security-assessment-tool.

7) *Explain any special circumstances that would cause the information collection to be conducted in a manner inconsistent with guidelines*

There are no special circumstances with this collection.

8) *Consultation*

60 Day Comment Period: A 60-day public notice for comments was published in the Federal Register on December 17, 2012 at 77 FR 74678. The Department received two relevant comments:

(1) The first comment was from the Institute of Makers of Explosives and requested that Department correct a citation in the Top Screen Questions Document (version 1.3). The Department responded in the 30 day notice that an updated document (version v2.8) was published in January of 2009 and is available on the DHS website.

(2) The second comment was from the American Chemistry Council and had several points some of which resulted in changes to the burden estimates in the 30-day notice for CSAT.

a. ACC correctly identified two calculation errors.

b. ACC did not agree with the estimated amount of time the Department estimated for a respondent to complete and submit a Top Screen, SVA/ASP, and an SSP/ASP. ACC conducted a survey and provided their own estimates for the Department's consideration. The Department revised its estimates in the 30-day notice by increasing the assumption about how long a respondent spends an average from:

i. Two hours to four hours in preparation outside of CSAT for every hour logged into CSAT for the Top Screen and SVA/ASP
ii. 4.5 hours to four hours in preparation outside of CSAT for every hour logged into CSAT for the SSP/ASP.

30 Day Comment Period: A 30-day public notice for comments was published in the Federal Register on March 18, 2013 at 78 FR 16694. No comments were received.

9) Explain any decision to provide any payment or gift to respondents

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

10) Describe any assurance of confidentiality provided to respondents

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) P.L. 109-295 further clarifies 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."

(3) The Department published a System of Records Notice which covers this collection on December 29, 2006 (71 FR 78446).[1] The Department will develop and publish additional System of Record Notices as necessary.

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

[1] http://edocket.access.gpo.gov/2009/E9-23513.htm

Department will use 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) Additional justification for any questions of a sensitive nature

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

12) Estimates of reporting and recordkeeping hour and cost burdens of the collection of information

The annual total estimate for reporting, recordkeeping and cost burden under this collection is $25,497,500. Individual burden estimates vary by instrument and are summarized in the table below:

Table 2: Instrument Burden Estimate

Instrument	# of Respondents	Responses per Respondent	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	0.17	2,250		219,300
User Registration	625	1	2	1,250		107,500
TS	2,500	1.5	11.25	42,500		3,655,000
SVA/ASP	740	1.5	65	72,200		6,212,900
SSP/ASP	486	1.5	225	164,100	1,191,400	15,302,800

13) Estimates of annualized capital and start-up costs

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

14) Estimates of annualized Federal Government costs

The annual cost of this collection is estimated to be $14M

15) Explain the reasons for the change in burden

- 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 2009 to December 2011.
- Decrease in the average annual burden as a result of the agency's discretion to remove the CVI Training and Authorization instrument from this collection
- Increase of the recordkeeping costs as a result of a correction.

16) For collections of information whose results are planned to be published for statistical use, outline plans for tabulation, statistical analysis and publication

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

17) Explain the reasons for seeking not to display the expiration date for OMB approval of the information of collection

The expiration date will be displayed in the instruments.

18) Explain each exception to the certification statement

No exceptions have been requested.