Supporting Statement A
Chemical Security Assessment Tool (CSAT)
OMB Control Number 1670-0007

A. JUSTIFICATION

1) Circumstances that make the collection of information necessary.

Section 550 of P.L. 109-295 (Section 550) directed the Department of Homeland Security to promulgate and enforce regulations to enhance the security of the nation's high risk chemical facilities. On April 9, 2007, the Department issued an Interim Final Rule, implementing this statutory mandate at 72 FR 17688. Section 550 requires a risk-based approach to security. To facilitate this approach, the Department is employing a risk assessment methodology and Information Technology tool known as the Chemical Security Assessment Tool (CSAT). The CSAT is a series of six public web-based computer applications: User Registration, Top-Screen, Security Vulnerability Assessment (SVA), Site Security Plan (SSP), Personnel Surety, and Chemical-terrorism Vulnerability Information (CVI) Authorization. Each of these computer applications represents a collection. In addition, the rule allows separate Alternative Security Programs (ASPs) to be provided by a facility in lieu of the SVA or the SSP under specific circumstances. These ASPs can be in any form preferred by the submitting facility, but must meet the information collection requirements in the SVA and SSP sections of the Interim Final Rule. The CSAT Helpdesk constitutes another collection associated with this program but not managed by the CSAT tool.

Section 550 required the Department to promulgate interim final regulations no later than six months from the date of enactment of the statute (i.e., April 4, 2007). Due to that short statutory deadline, the CSAT applications and information collections are in different development stages. In early March 2007, when DHS submitted the IFR to OMB, only two of the collections (User Registration and Top-Screen) were ready for PRA review. As of mid-May 2007, four of the collections (Helpdesk, User Registration, Top-Screen, and Chemical-terrorism Vulnerability Information Authorization) were sufficiently complete for PRA review. As of early October 2007 two additional collections are sufficiently complete for PRA review: (1) the Security Vulnerability Assessment and industry-created and provided Alternative Security Program submitted in lieu of the Security Vulnerability Assessment, and (2) the Site Security Plan or the industry-provided Alternative Security Program submitted in lieu of the Site Security Plan. The Personnel Surety collection remains in the early stages of development and DHS is still working through the requirements definition stage of the IT development lifecycle.

Scope: The six (6) separate collection requirements associated with CSAT are outlined below.

(A) CSAT Helpdesk (not publicly accessible from the internet)	(No Change)
(B) Chemical-terrorism Vulnerability Information (CVI) Authorization	(No Change)
(C) CSAT User Registration	(No Change)
(D) CSAT Top Screen	(No Change)
(E) CSAT Security Vulnerability Assessment & ASP	(No Change)
(F) CSAT Site Security Plan & ASP	(No Change)

This CSAT information collection supports the following strategic goals:

Department of Homeland Security
- Prevention of terrorist attacks against the nation

Office of Infrastructure Protection
- Identifies and Secures Chemical Facilities against Terrorism

Chemical Security Assessment Tool
- Facilitates self-assessment by facilities of their vulnerabilities

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 identification of high risk facilities and critical assets; the determination of the risk tiers of the facilities; the identification and assessment of security vulnerabilities at the facilities; the identification, implementation and/or approval of security measures at the facilities; and/or the protection of sensitive information that would, if disclosed, substantially assist terrorists in planning and targeting the facilities.

(A) CSAT Helpdesk

This collection of information was approved under an emergency request to OMB on 06/6/07. It expires on 2/29/08. There are no changes to this instrument as part of this revision.

SYNOPSIS OF COLLECTION: Pursuant to 6 CFR 27.210(b), the Department will provide technical assistance and consultation to chemical facilities. One of the methods through which the Department will provide such assistance is through a CSAT Helpdesk. Through the CSAT Helpdesk, the Department will provide technical assistance for the use of the CSAT computer applications.

The Department will manage the CSAT Helpdesk through Oak Ridge National Laboratory. Oak Ridge National Laboratory maintains the Helpdesk both on site and with a subcontracted third party. Chemical facilities that need technical assistance or consultation can contact the CSAT Helpdesk via phone or e-mail (csat@dhs.gov).

(B) Chemical-terrorism Vulnerability Information (CVI) Authorization

This collection of information was approved under an emergency request to OMB on 06/6/07. It expires on 2/29/08. There are no changes to this instrument as part of this revision.

SYNOPSIS OF COLLECTION: Pursuant to 6 CFR 27.400(e) (3), the Department may "make an individual's access to CVI contingent upon … procedures and requirements for safeguarding CVI that are satisfactory to the Department." In order to provide individuals with access to CVI, the Department will require individuals to undergo training about CVI. Specifically, the Department will train individuals on the appropriate maintenance, safeguarding, making, disclosure, and destruction of CVI.

The CVI training will be targeted primarily towards (1) individuals employed or contracted by chemical facilities and (2) Federal, State, local employees and contractors. The Department will need to maintain a record that an individual has completed this training and is authorized to access CVI.

To obtain CVI authorization, an individual will complete a web-based application. Upon completion of the application, the system will transmit the individual's information to the Department, so that the Department can determine authorization and subsequently maintain a list of authorized people who have access to CVI data. Authorization for access to CVI does not constitute "need to know." The individual will sign a Non-Disclosure Agreement (NDA) by selecting a series of boxes next to each paragraph of the NDA and providing basic identifying information.

Chemical-terrorism Vulnerability Information (CVI) is a new Sensitive But Unclassified designation authorized under P.L. 109-295 and implemented in 6 CFR 27.400. CVI came into existence on June 8, 2007, when 6 CFR Part 27 became effective. It is essential to provide training in order to protect the sensitive data that will be provided to the government.

(C) CSAT User Registration

This collection of information was approved under an emergency request to OMB on 06/6/07. It expires on 2/29/08. There are no changes to this instrument as part of this revision.

SYNOPSIS OF COLLECTION: CSAT User Registration is completed by individuals at a chemical facility who will be involved in the development of the Top-Screen, SVA or substituted ASP, SSP or substituted ASP, or Personnel Surety applications of CSAT. The CSAT User 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 User Registration form, the system generates an Acrobat PDF document (DHS Form 9002) and print request. All individuals requesting or providing authority to access CSAT are listed on the printed document that they sign and date. The individual should send the completed form via fax to 866-731-2728 or via mail to Chemical Security Compliance Division, ATTN: CSAT User Registration, Department of Homeland Security, Building 5300, MS 6282, and P.O. Box 2008, Oak Ridge, TN 37831-6282.

(D) CSAT Top-Screen

This collection of information was approved under an emergency request to OMB on 06/6/07. It expires on 2/29/08. There are no changes to this instrument as part of this revision.

SYNOPSIS OF COLLECTION: The primary purpose of CSAT Top Screen is to help DHS obtain an overview of security issues presented by the nation's chemical facilities, including helping to identify covered facilities under 6 CFR Part 27.

To identify covered facilities, DHS will have to gather 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."

In particular, 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.

(E) Site Vulnerability Assessment & Alternative Security Program submitted in lieu of the Site 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 classified 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.

Therefore, DHS requests a single approval for the collection of information for SVAs and ASPs submitted in lieu of an SVA.

ATTACHMENT: CSAT SVA form (DHS Form 9015)

(F) CSAT Site Security Plan (SSP)

In 6 CFR Part 27.225(a) DHS 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]dentify 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

3) Consideration of the use of improved information technology.

The overall paperwork burden associated with this information collection will be reduced as a result of the web-enabled interface of the user data submission process. Typically

users can type in their information and submit it over the Internet, cutting down on the overall time associated with paper-based, manual processes (including traditional postal services). The systems are designed to dynamically respond to user input and thereby only request the minimum amount of necessary data that results in the correct conclusion for each facility.

4) Efforts to identify duplication.

The CSAT is a new tool, which the Department has developed 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.

The burden imposed on small businesses is alleviated in instances when certain smaller facilities are not deemed high risk, and therefore would be exempted from the regulation and registration processes. Burden is further reduced by CSAT's ability to dynamically generate questions based on the user's input so that only the minimum number of questions answered is required.

6) Consequences to the Federal program if collection were conducted less frequently.
This is the first nation-wide comprehensive review of the chemicals stored and produced by each facility. 6 CFR Part 27.210 provides specific submission schedules for chemical facilities data entry into the Top Screen, SVA and SSP. CSAT is online and is available for user registration, training or data entry 24 hours each day every day of the week. The Helpdesk is available Monday through Friday 7AM – 7PM EST business days. CVI training is only required once and again only if the individual's status changes.

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. Explicit guidelines are set forth in 6 CFR 27.210.

8) Consultation.

On November 23, 2007, the Department published a 60 Day Federal Register Notice (72 FR 65757).

One comment was received. The comment stated that User Registration took 8 hours, instead of the estimated 60 minutes. A response letter was sent January 31, 2008, referencing the several thousand surveys of CSAT users that support an average time burden of 60 minutes.

On January 28, 2008, the Department published a 30 Day Federal Register Notice (73 FR 4886)

There were no comments 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 new 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 on December 29, 2006 (71 FR 78446). DHS will develop and publish additional System of Record Notices as necessary.

(4) The Helpdesk completed an initial Certification and Accreditation test to a satisfactory level. The Department reserves the right to audit the Helpdesk facilities and infrastructure at any time. There are physical measures in place to ensure that only authorized individuals have access to the Helpdesk call center. The same access restrictions are part of the electronic infrastructure.

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 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 elements of the CSAT system described in this application do not request any information to personally sensitive data. The CSAT system requests limited personally identifiable information for registration purposes only. Top-Screen questions may require the disclosure of proprietary business information.

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

- Individuals may either call into the Helpdesk or contact the Helpdesk through email. The total estimated annual number of responses is **20,800**.
- Individuals will need to obtain CVI authorization only once. Thus, the total annual responses in the first year are expected to be approximately **40,000**. This is because although all CSAT users must obtain CVI authorization and sign Non-Disclosure Agreements, not all CVI-authorized individuals will need to access CSAT.
- The total respondents for the User Registration and Top-Screen are estimated to be approximately **40,000**. No facility can access the Top-Screen portion without completing the User Registration portion. Because each respondent will be entering information for each part of the system, there will technically be 80,000 responses.
- Individuals needing to complete either the SVA or ASP are estimated to expend 250 hours per a facility for a total of 750,000 total hours.
- Individuals who need to complete the SSP or ASP are estimated to consume 200 hours per a facility to complete the questionnaire with a total burden of 10,000 hours for all facilities.
- The total hour burden for completing the User Registration, Top Screen, obtaining CVI authorization (including calls to the Helpdesk), SVA and SSP is **2,037,200** hours.

- The total annual burden cost estimate is: **$229,915,100**.
- The total contractual cost for the government for this system is: **$10,000,000**.

Table A.12: Estimated Annualized Burden Hours

Information Collection	Form Name and / or Form Number	No. of Respondents	No. of Responses per Respondent	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)
Help Desk	DHS 9010	20800	1	15 min	5200
User	DHS 9002	40000	1	1 hour	40000

Registration					
Top Screen	DHS 9007	40000	1	30.3 hours	1212000
CVI User Training	DHS 9012	40000	1	30 min	20000
SVA	DHS 9015	3000	1	250 hours	750000
SSP	DHS 9019	50	1	200 hours	10000
Total		143,850			2,037,200

A. Estimated Burden for the CSAT Helpdesk (DHS Forms 9009 & 9010)

Time Required for Each Individual Respondent (Minutes)	15
Annual Hours Burden (Hours x 20,800 respondents)	5,200

The Department estimates that the Helpdesk will receive 400 requests for assistance per week. Of these 400 requests, we believe 95% will be phone calls and 5% will be emails. We estimate that the time required for each contact will be approximately 15 minutes. This includes follow-up calls and emails. At this rate, there will be approximately 20,800 calls and emails per a year, equating to 5,200 hours.

B. Estimated Burden for the CVI Authorization (DHS Form 9012)

Time Estimated for Individual (Minutes)	30.0
Annual Hours Burden (Hours x 40,000 Individuals)	20,000

The Department estimates that CVI authorization will take 30 minutes per individual. This includes the time it takes to complete the Non-Disclosure Agreement. The Department anticipates there will be 40,000 individuals that will obtain this authorization.

C. Estimated Burden for User Registration (DHS Form 9002)

Time Required for Each Facility (Hours)	1
Annual Hours Burden (Hours x 40,000 facilities)	40,000

D. Estimated Burden for the Top-Screen (DHS Form 9007)[1]

Time Required for Each	30.3

[1] Numbers may not sum to total due to rounding.

Facility (Hours)	
Annual Hours Burden (Hours x 40,000 facilities)	1,212,000

Facilities will have different burden rates due to the size and complexity of the facility. The Top-Screen is designed to dynamically respond as the user answers different questions. The Department estimates that, on average, it will take 30.3 hours to complete the Top-Screen, thus resulting in an estimated total burden of 1,212,000 hours.

E. Estimated Burden for the Site Vulnerability Assessment DHS Form 9015 (06/07)

Time Required for Each Facility (Hours)	250
Annual Hours Burden (Hours x 3,000 facilities)	750,000
Cost for Each Facility	$58,500,000

The SVA is designed for those facilities that are determined to be a Tier 1, 2 or 3. Facilities may also upload an Alternative Security Program from their corporate files to answer the questions addressed in the SVA. Tier 4 facilities are not required to submit SVA documentation

F. Estimated Burden for the Site Security Plan (DHS Form)

Time Required for Each Facility (Hours)	200
Annual Hours Burden (Hours x 50 facilities)	10,000
Cost for Each Facility	$750,000

If it is easier for the facility to answer the questions with their own internal documentation, the facility may upload an Alternative Security Program document.

13) Estimates of annualized capital and start-up costs.

There are no annualized capital or start-up costs for this information collection. It is assumed that all participants will already have the computer hardware and web browser.

14) Estimates of annualized Federal Government costs.

The cost to develop and implement the entire CSAT system is estimated to approximately $10M. Annual estimates for the seven information collections can not yet be estimated, because the system is still under development.

15) Explain the reasons for the change in burden.

There has been no change in burden.

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 system.

18) Explain each exception to the certification statement.

No exceptions have been requested.