CSAT Site Security Plan

Instructions

May 2009

Version 1.0

Homeland Security

Table of Contents

Note to Users

This document provides instructions to facilities for completing and submitting the Chemical Security Assessment Tool (CSAT) Site Security Plan (SSP) in accordance with requirements of the Department of Homeland Security's (DHS or the Department) Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27. The CFATS rule authorizes DHS to collect information from chemical facilities on a broad range of topics related to the potential consequences of, or vulnerabilities to, a terrorist attack or incident. The CSAT SSP is one method DHS uses, as provided by 6 CFR § 27.225, to gather such information from high-risk facilities.

Any facility that receives a Final Notification Letter from DHS, designating it a high-risk facility, must complete an SSP or an Alternative Security Program (ASP) in lieu of an SSP. The CSAT SSP tool collects information from covered facilities regarding existing and - if a covered facility so chooses - planned and proposed security measures related to the CFATS Risk-Based Performance Standards (RBPS). See 6 CFR § 27.230. Facilities are required to list and/or describe existing security measures as part of their CSAT SSP submissions. Existing and planned security measures which each covered facility describes or lists in its CSAT SSP submission may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. However, the CSAT SSP tool will also provide facilities the opportunity to identify certain security measures in the SSP but then exclude them from evaluation of the SSP. Of course, if a facility chooses not to provide information about an existing or planned measure that is relevant to the satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Under CFATS, any high-risk facility (assigned to Tier 1, 2, 3, or 4) may choose to submit an ASP in lieu of an SSP, as provided in 6 CFR § 27.235. This document also provides instructions on submitting an ASP. Even if a facility plans to upload an ASP, the facility must answer all questions in the General and Facility Operations sections of the SSP before uploading its ASP. The General and Facility Operations sections address basic details of a facility's operations as well as its on-site and off-site response capabilities.

All examples in these instructions are illustrative and merely intended to highlight specific points within the CSAT SSP tool. Each facility must carefully consider its own unique characteristics and circumstances to determine the relevance and appropriateness of each example. DHS will not disapprove an SSP based on the presence or absence of a particular security measure.

CSAT users may call the CSAT Help Desk with questions regarding the CSAT SSP tool. Contact information for the CSAT Help Desk is provided in the "Getting Additional Help" section of these instructions. CSAT users may also click on the left-hand menu bar button labeled ***Help*** on the menu on the left where the SSP tool provides links for additional guidance material, including the DHS RBPS Guidance Document when available.

Introduction

Section 550 of the DHS Appropriations Act of 2007, Pub. L. 109-295 (Sec. 550 or the Act), authorizes DHS to regulate the security of high-risk chemical facilities. The CFATS Interim Final Rule (IFR), 6 CFR Part 27, was published on April 9, 2007, to implement the Act. See 72 FR 17688. In addition, on November 20, 2007, DHS published a final Appendix A to CFATS. See 72 FR 65396.

Under CFATS, any facility that possesses any chemical of interest (COI) in an amount at or above the applicable Screening Threshold Quantity (STQ) for that chemical, as listed in Appendix A to CFATS, must complete and submit certain screening information, called a Top-Screen, to DHS. To do so, the facility must first register with DHS for access to CSAT. After reviewing the Top-Screen, the Department will notify the facility in writing of its initial determination as to whether the facility is considered high-risk.

If the Department initially determines that the facility is high-risk, the Department also will notify the facility of its preliminary placement in a risk-based tier (Tier 1, 2, 3 or 4) pursuant to 6 CFR § 27.220(a). Facilities initially determined to be high-risk are required to complete a Security Vulnerability Assessment (SVA) to identify the critical assets at the facility and to evaluate the facility's security vulnerabilities in light of the security issues identified in its preliminary tier notification letter from DHS. Each facility preliminarily placed into Tier 1, 2 or 3 must use the CSAT SVA tool to complete its SVA. See 6 CFR § 27.215. Each Tier 4 facility may use the CSAT SVA tool to complete an SVA or may submit an Alternative Security Program (ASP) in lieu of an SVA, as provided by 6 CFR § 27.235.

Following submission and analysis of its SVA or ASP, DHS will either confirm that the facility is high-risk or inform the facility that it is not high-risk and is no longer subject to CFATS, barring a change in the facility's circumstances. For facilities confirmed to be high-risk, DHS will provide each facility a Final Notification Letter specifying the final facility tier, applicable COI and security/vulnerability issue(s). The facility then must complete and submit an SSP under 6 CFR § 27.225 (or an ASP in lieu of a SSP, as provided by 6 CFR § 27.235) that satisfies the applicable RBPS by the date specified in its Final Notification Letter.

These instructions apply only to the CSAT SSP tool.

SSP Instructions: The SSP Process

The CSAT SSP tool follows a logical data collection process. First, a facility provides basic facility information. Second, a facility describes its security measures applicable across the entire facility. If a facility also implements specialized security measure for particular assets, the facility then describes such assets and their unique security measures. As a starting point for describing asset-specific security measures, the asset-specific portions of the SSP tool will be pre-populated with any facility-wide security measures already selected by the user. By collecting information on facility-wide and asset-specific security, DHS will obtain an accurate picture of all the security measures a high-risk facility employs or plans to employ in satisfying the CFATS RBPS.

The SSP tool will automatically pre-populate certain data fields.

Organization of these Instructions

These instructions are generally organized in the same order as the questions and sections appearing in the CSAT SSP tool itself.

Section 1 covers Getting Started.

This includes instructions on signing into the SSP tool, instructions on navigating the SSP tool, and instructions on saving and validating facility data.

Section 2 covers General Facility Information.

The instructions provided in Section 2 will assist you in completing the tab marked *General* found in the Navigation Menu. In this section, DHS requests information on facility name, address, SVA completion information, North American Industrial Classification System (NAICS) code, Dun & Bradstreet (DUNS) number, Environmental Protection Agency Risk Management Plan (EPA RMP) facility identification number, as well as owner and operator names.

Section 3 covers Facility Operations.

The instructions provided in Section 3 will assist you in completing the tab marked *Facility Operations* found in the Navigation Menu. In this section, DHS requests information on facility personnel contact information, including phone numbers, emergency management and response information, total number of personnel working at each facility, and hours of operation.

Section 4 covers Facility Security Measures.

The instructions provided in Section 4 will assist you in completing the tab marked *Facility Security Measures* found in the Navigation Menu. This includes addressing those RBPS that always apply at the facility-wide level and then answering questions about existing security measures relevant to those RBPS and any other RBPS that the facility wishes to address at the facility-wide level. The facility may also provide information on any planned or proposed security measures relevant to each RBPS. (Only planned security measures are considered in the formal evaluation of the facility's submitted SSP. Proposed security measures are not considered as part of formal evaluation.) This section will also provide facilities the opportunity to propose that certain existing and/or planned security measures not be considered by DHS in evaluating their SSPs for approval. Of course, if a facility chooses not to provide information about an existing or planned measure that is relevant to satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Section 5 covers Asset Security.

The instructions provided in Section 5 will assist you in completing the tab marked *Asset Security* found in the Navigation Menu. A facility may apply specialized security to a

particular asset (which may include restricted areas and critical/target assets) or group of assets at the facility. This section will provide instructions to enable a facility to identify existing asset-level security measures relevant to a particular RBPS. The facility may also provide information on any asset-specific planned or proposed security measures. (Only planned security measures are considered in the formal evaluation of the facility's submitted SSP. Proposed security measures are not considered as part of formal evaluation.) This section will also provide facilities the opportunity to propose that certain existing and/or planned security measures not be considered by DHS in evaluating their SSPs for approval. Of course, if a facility chooses not to provide information about an existing or planned measure that is relevant to satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Section 6 provides instructions for validating, reviewing, and submitting the SSP to DHS.

For easy identification of questions, each question number appearing in brackets in the text below corresponds to the same question number in the SSP tool. For example, "[Q:3.0-13871]" appears below the question in the SSP tool requesting Facility Type. This question number also appears in the associated explanation in these instructions. Question numbers are also useful references for users contacting the CSAT Help Desk.[1]

CSAT User Access Roles

In order to access the CSAT tools, a facility must register with DHS. Facilities that have submitted CSAT Top-Screens have already registered and been assigned the user roles listed below. For preparation of the CSAT SSP, individuals retain the user access roles previously assigned to them for completion of the Top-Screen and SVA.

For each facility, a variety of individuals can be authorized to use CSAT. Each registered individual will be assigned a specific role, with access rights and privileges based on that role unless roles are transferred as indicated below. The roles (Preparer, Submitter, Authorizer, and Reviewer) are defined in the CSAT User Registration Guide. Facilities may assign and/or transfer responsibility among individuals through the CSAT system. Information on how to assign and/or transfer or consolidate roles is available in the CSAT User Registration Guide and Account Management Guide available at http://www.dhs.gov/xprevprot/programs/gc_1169501486197.shtm. Beyond the access rights and privileges outlined in the CSAT User Registration Guide, it is each facility's responsibility to organize and manage the individuals and teams of individuals contributing to its CFATS compliance. This is especially true during the completion and submission of the SSP, which will likely involve multiple users.

Given that the SSP tool allows multiple Preparers to enter information, it is important to note that when the Preparer sends the SSP to the Submitter for review, the Preparer will no longer be able to edit the information in the SSP unless the SSP is returned to the Preparer by the Submitter for revision. When the Submitter has access to the SSP, he/she may revise the information contained therein. Once the Submitter

[1] The CSAT Help Desk has a toll-free number that CSAT users can call with questions regarding CSAT, including the CSAT SSP tool. The CSAT Help Desk can be reached at 866-323-2957 between 7 a.m. and 7 p.m. (Eastern Standard time), Monday through Friday. The CSAT Help Desk is closed on Federal holidays.

transmits the SSP to DHS, it is no longer accessible to the facility or its designated Preparer, Authorizer, Reviewer, or Submitter. The Authorizer has no role in the on-line review of the SSP unless he or she is also the Preparer or Submitter. The CSAT Help Desk can provide further information on users and user roles for purposes of completing the SSP.

If DHS rejects an SSP that a facility has submitted or if a facility needs to repeat the SSP process, the facility must re-enter all the information into the SSP tool, because the system currently does not retain the SSP after submission. Therefore, a facility should retain a copy of its completed SSP. See Section 6 for directions on how to save and/or print a copy of the SSP before it is submitted to DHS.

Preparing to Begin the SSP: Relevant Information and Resources

Prior to beginning an SSP, the facility may wish to collect and review the information below. Verifying the accuracy and completeness of such data prior to starting the SSP will allow for quicker completion.

- The CSAT SSP instructions;
- A copy of the CFATS regulation, 6 CFR Part 27, including Appendix A (the DHS COI list), available at http://www.dhs.gov/chemicalsecurity;
- A copy of the DHS Final Notification Letter;
- A copy of the Chemical-terrorism Vulnerability Information (CVI) Procedures Manual regarding protection of CVI, available at http://www.dhs.gov/chemicalsecurity;
- A copy of the Risk-Based Performance Guidance Document when available;
- A copy of any recent SVA or SSP completed by the facility;
- Any existing facility security plan, including facility and asset level security measures, procedures, or policies;
- Any security measures in the planning, procurement and/or proposal stages;
- Any existing facility emergency response plans;
- Off-site emergency response contact and capabilities information;
- Local and Federal law enforcement contact and capabilities information;
- Any security drill and exercise records;
- Any special security and response capabilities:
- Any existing mutual assistance group(s) (MAG) and mutual aid agreement(s) information;
- Number of full- and part-time employees and contractors, and number and duration of work shifts;
- Facility diagram;
- Information on any facility personnel background check or company background check procedures;
- Information on any "Know Your Customer" or customer validation procedures.

Chemical-terrorism Vulnerability Information

Chemical-terrorism Vulnerability Information (CVI) refers to the information protection requirements and procedures established by the CFATS rule to protect sensitive information submitted for purposes of complying with CFATS. See 6 CFR § 27.400. Each completed SSP or ASP (and every copy of each SSP or ASP) is a CVI document. In addition, each partially completed SSP is CVI. Therefore, every CSAT user must be a CVI Authorized User (i.e., must complete CVI training) prior to entering information into the CSAT SSP tool. CVI training addresses how to protect information submitted through the CSAT SSP tool, and to whom and under what circumstances such information may be disclosed. The DHS CVI training is available from a link on this page (*Training for Chemical-terrorism Vulnerability Information*): http://www.dhs.gov/xprevprot/programs/gc_1185556876884.shtm. **A user will not have access to the CSAT SSP tool until the user has completed CVI training and is a CVI authorized user.**

For more details regarding what information is and is not CVI and regarding the procedures for protecting CVI, please refer to the DHS CVI Procedures Manual, which is available at http://www.dhs.gov/chemicalsecurity.

Getting Additional Help

More details on 6 CFR Part 27, information regarding CVI, and other related information is available on the DHS website at http://www.dhs.gov/chemicalsecurity.

For answers to specific technical or substantive questions related to the CSAT SSP, individuals may contact the CSAT Help Desk. The CSAT Help Desk has a toll-free number that a CSAT user can call with questions regarding CSAT, including the SSP tool. The CSAT Help Desk can be reached at 866-323-2957 between 7:00 a.m. and 7:00 p.m. (Eastern Standard Time), Monday through Friday. The CSAT Help Desk is closed on Federal holidays.

1.0 Getting Started

1.1 Sign-in Screen

The Final Notification Letter that DHS sends to each facility will have instructions for accessing the CSAT SSP tool. The CSAT tool will prompt the user to enter his or her username and password.

Once you have logged in, a screen will appear which lists each registered facility and the associated documents to which you have access (including Top-Screens and SVAs). At this point, you have three options: (1) access the SSP tool for a given facility, (2) manage user roles for any of the facilities displayed; and/or (3) update facility information with a new name or address.

To access the SSP tool for a given facility, click the *Edit/Review* button.

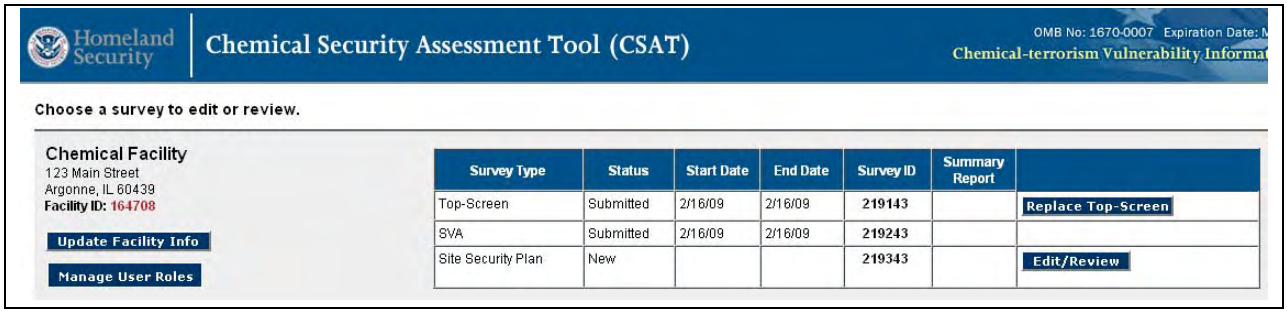

Figure 1-1 – Choose Facility

1.1.1 Manage User Roles

To manage the user roles, Submitters, Preparers, and Authorizers can add Reviewers or Additional Preparers to an SSP by clicking on the *Manage User Roles* button.

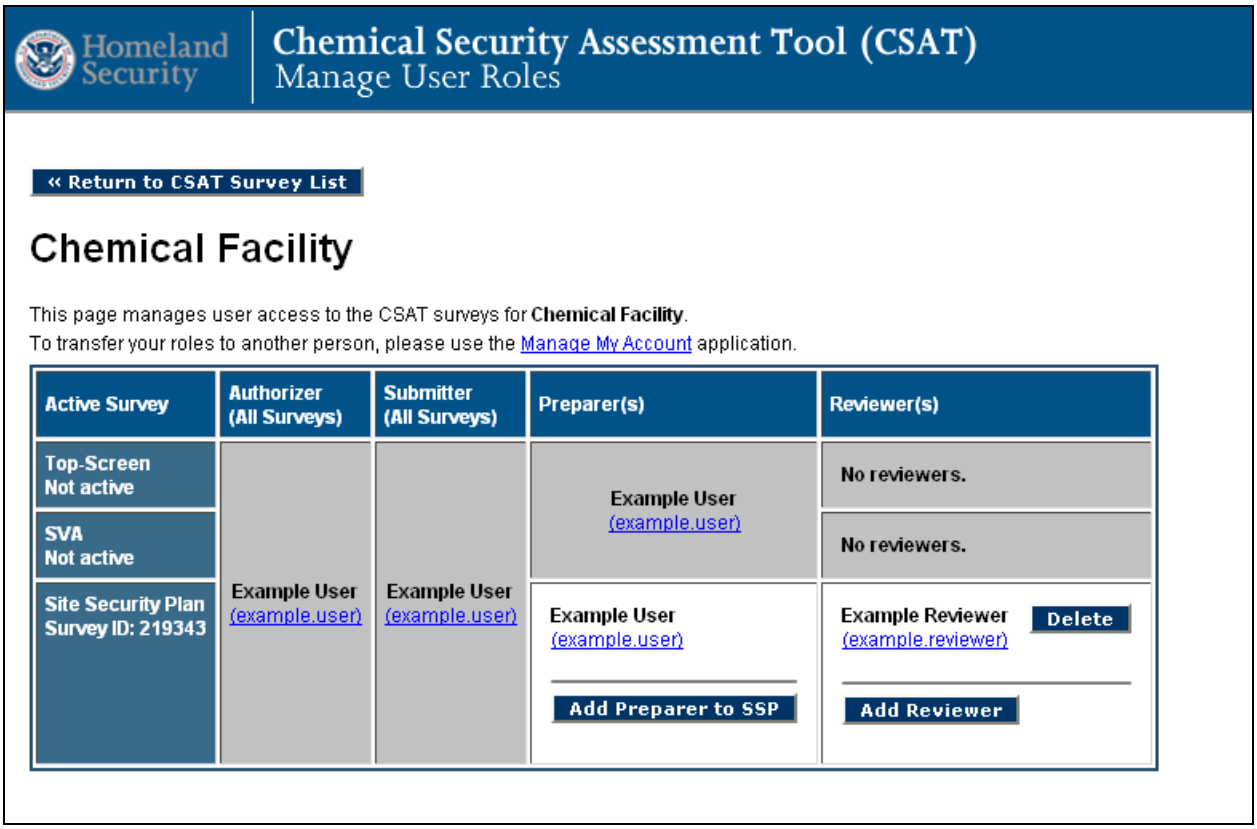

Figure 1-2 – Manage User Roles

Add/Delete Reviewer

Each reviewer added during the Top-Screen or SVA completion process for a given facility will be able to view the SSP for the same facility. To delete a reviewer, click the *Delete* button. To add a reviewer, click on the *Add Reviewer* button to the right of the survey for which you would like to add the reviewer. After clicking the *Add Reviewer* button, you will be directed to a screen asking whether you would like to grant reviewer access to an existing CSAT user or to a new CSAT user. Select the appropriate choice by clicking on the blue bar and entering the requested information.

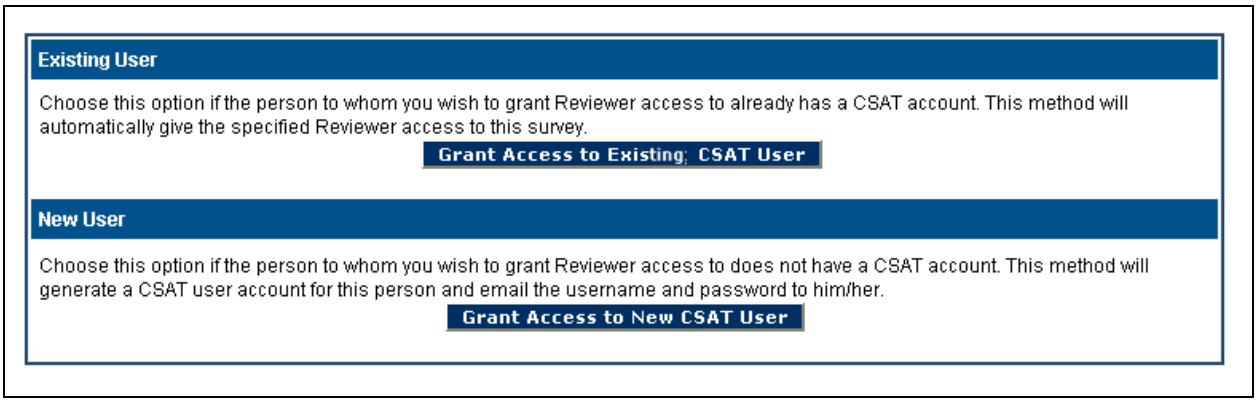

Figure 1-3 – Granting Reviewer Access

Note: Do not grant yourself Reviewer privileges if you are an Authorizer, Submitter, or Preparer. Doing so will disable all editing privileges.

To remove a Reviewer, the Authorizer will need to contact the Help Desk.

Add Preparer

To add additional preparers for an SSP, click the *Add Preparer to SSP* button. After clicking the button, you will be directed to a screen asking whether you would like to grant preparer access to an existing CSAT user or a new CSAT user. Select the appropriate choice by clicking on the blue bar and entering the requested information. Both options generate a PDF form that you will need to return the Help Desk for approval.

When multiple preparers are updating the same SSP, changes made by one will be visible to the others as soon as those changes are saved (by clicking *Save*, *Next* or *Back*).

1.1.2 Update Facility Information

To update facility information, including changing facility name or address, click on the *Update Facility Info* button. The address information presented on the Update Facility Information page is populated from the SVA application. Use the *Update Facility Information* button here, or in the SSP tool, to complete other facility information changes. See the Update Facility Information section later in these instructions for further description of the applicable fields.

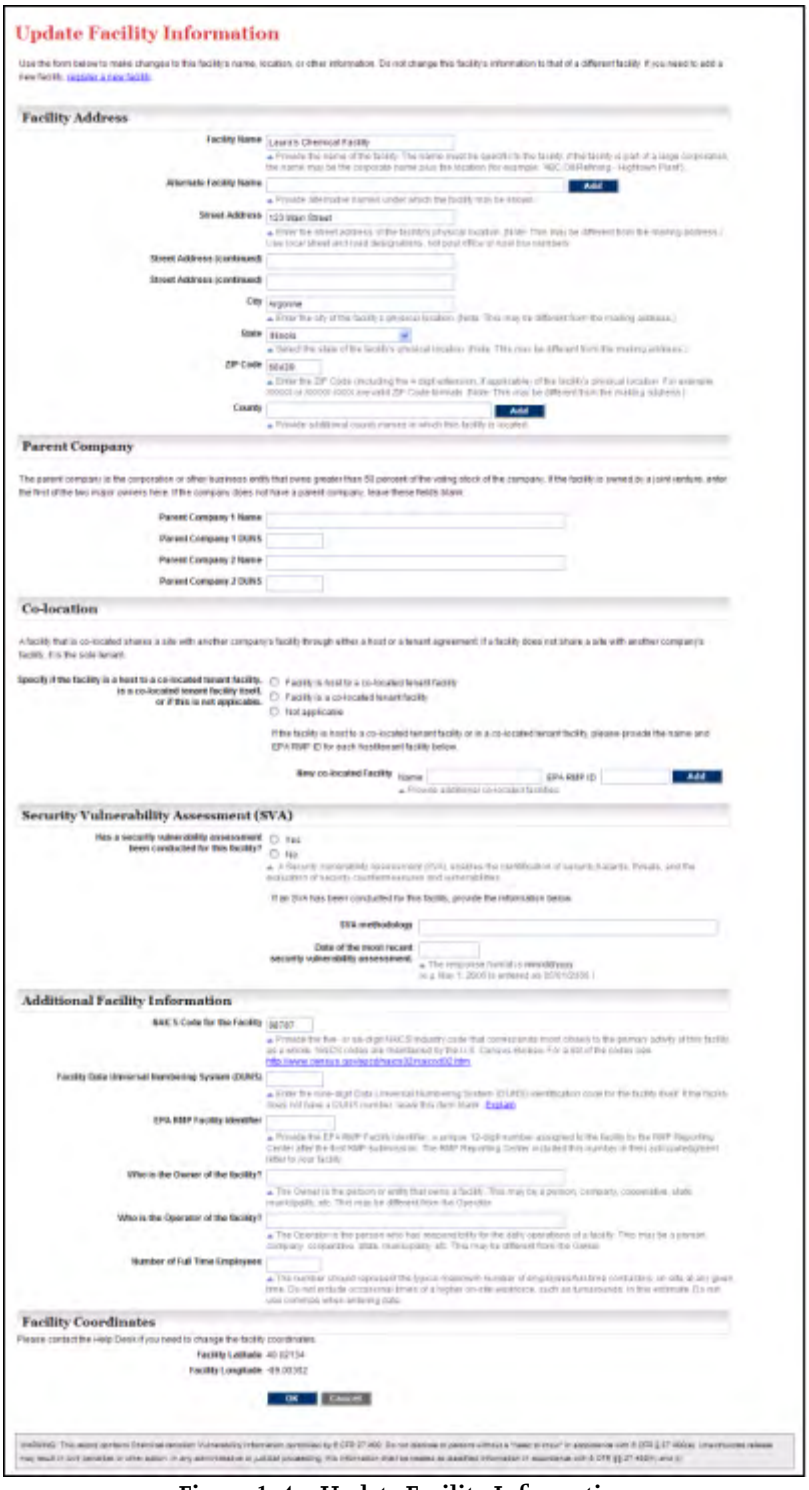

Figure 1-4 – Update Facility Information

Facility information can be updated from this screen. Do not use this screen to create a new facility. If a new facility needs to be registered, click the *register a new facility* text at the top of the screen. New facilities will be required to complete the entire CSAT process as outlined in the Introduction to these SSP tool instructions. Review for accuracy all of the information on this page, including the section on Security

Vulnerability Assessment (SVA) and enter any corrections in the appropriate boxes and click OK. A facility's coordinates (latitude/longitude) cannot be changed from within the SSP application. Contact the Help Desk to process a latitude/longitude change.

1.2 Navigating within the Tool

Navigation within the SSP tool is straightforward. You can navigate to the next and previous screens by using the ***Next*** and ***Back*** buttons on the screen.

Figure 1-5 – SSP Back, Save, and Next Buttons

Using the *Next* and *Back* buttons will automatically save the information entered on the current page. If you are entering information and not leaving the page, click the *Save* button to retain the information.

> **Warning: Do not use the *Back* button (or arrows) in your web browser.** Using the browser's navigation buttons can result in the loss of data.

A navigational menu appears on the left side of the screen (see Figure 1-6). You can also navigate through the SSP by clicking on the desired topic in that menu. Sections of the SSP will be highlighted (and become selectable) only after each section has been sequentially accessed (i.e., you can move backward through the system by selecting previously completed sections, but cannot jump forward). **Please note that if you return to a section of the SSP that you previously completed, you will need to review all the subsequent pages of the SSP** (using the *Next* button on each page). That is, when you jump back to a previous section, all preceding sections will become un-highlighted and you will be required to page through all the subsequent pages of the SSP tool. This is necessary because the SSP tool adapts the pages presented for completion based on answers on previous pages and a change within one section might require you to answer additional/different questions later.

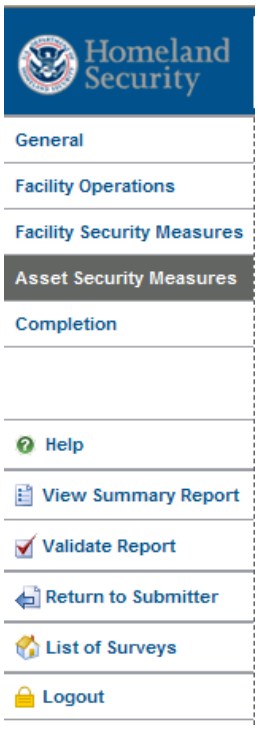

Figure 1-6 – SSP Navigational Menu

On some screens, you may need to include additional rows of text to complete the response to a question. If you need more than one text field, you should use the ***Add*** button to add a row. The ***Delete*** button can be used to delete a row or an entry.

Figure 1-7 – SSP Add Button

Where further explanation of a response is required, a *Describe* button is provided. When a *Describe* button appears, click it to answer additional questions specific to that item. At the conclusion of these additional questions, you will be asked if the description is complete (via a check box). When you indicate that the questions are complete, you will return to the list of items. If you marked the item complete and all required questions were answered for that item, the item will be displayed with a green check mark icon. If you do not check the box to indicate that the questions are complete, or if any required questions were not answered, the item will be displayed with a yellow warning icon as a reminder that the item is incomplete. Figure 1-8 shows both a complete and an incomplete icon.

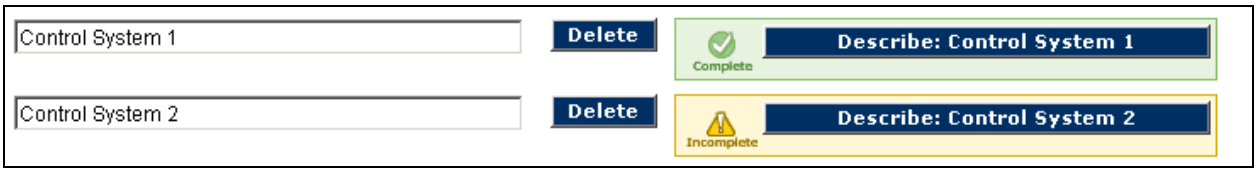

Figure 1-8 – SSP Describe Button

Your session will "time out" after 20 minutes if the system is not in use. You will need to log back in to restart the session. Data that has been entered and saved by clicking the ***Next*** or ***Save*** button will not be lost and the session will reopen on the same screen where the session "timed out."

1.2.1 Saving the Data

All data input in the SSP tool is saved automatically when you click the *Next*, *Save* or *Back* button. ***If you click the back or forward arrows in the Web browser, information may be lost.*** You can exit the program and return multiple times until the tool is complete, with data that has been saved during previous sessions available upon reentry into the SSP. As noted previously, if a session "times out" after 20 minutes, all data that has been entered will be saved if the *Next*, *Save* or *Back* button has been clicked.

Warning: Only use the *Next* and *Back* buttons in the SSP tool for navigation. This will help avoid losing information that has been entered.

1.2.2 Validating Data

Data validation is done at two different times. Some basic validation is completed before you can leave the screen and a more complete validation is done when you select *Validate Report* (this validation is also done automatically before submission).

Screen validation consists only of basic verification that entries have the correct format (e.g., that a phone number is numeric and formatted correctly).

Using the *Validate Report* option on the navigation menu will provide a more complete validation check. A validation error message will be displayed if required data input fields are skipped or completed incorrectly. The system allows you to return to the error and correct it. For example, if the facility security officer name and phone number are not entered, the following error report will be displayed. (See Figure 1-9). A link will direct you to the input area for correction.

The validation function will not find and highlight errors other than missing required data or logical errors (e.g., unrecognized characters such as commas or percent signs). Accordingly, the validation function should not be relied upon to ensure the SSP has been completed without errors. The Submitter is responsible for submitting accurate and correct information to the best of his or her knowledge.

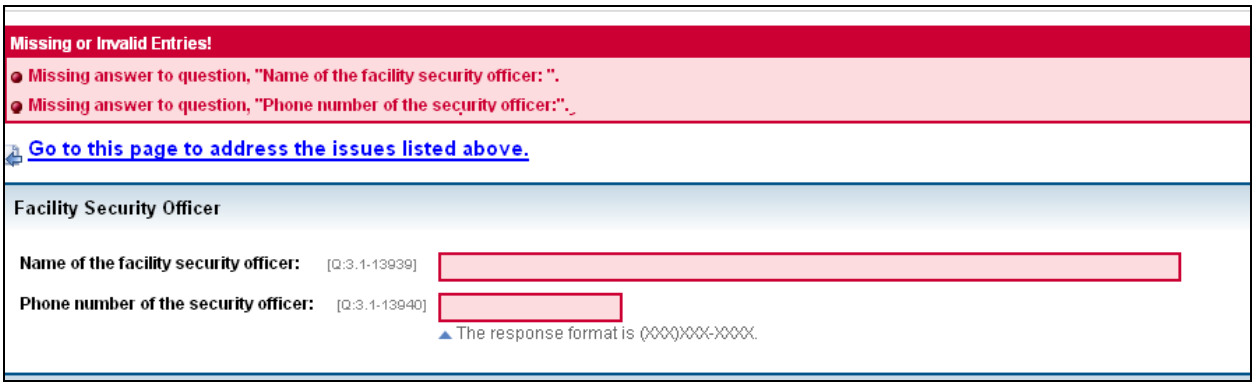

Figure 1-9 – Error Report Screen

1.3 "Pre-population" from SVA

If a facility is required to complete an SSP, some required information will be pre-populated from the facility's SVA. That means that CSAT will provide answers to certain questions based on information that the facility previously submitted to DHS in its SVA. If pre-populated information is inaccurate, the facility must phone the Help Desk and update the information in the SSP tool using the *Update Facility* button. (See Section 2.0 below.) The facility may also want to consider reviewing previous documents.

2.0 General Facility Information

To begin an SSP, the facility must provide the information requested on the General screens wherever the answers to the questions have not been pre-populated.

As appropriate, facility information in the SSP tool will be pre-populated using data from the facility's Top-Screen and SVA. This information should be reviewed. If updates are necessary, click on the *Update Facility Info* button.

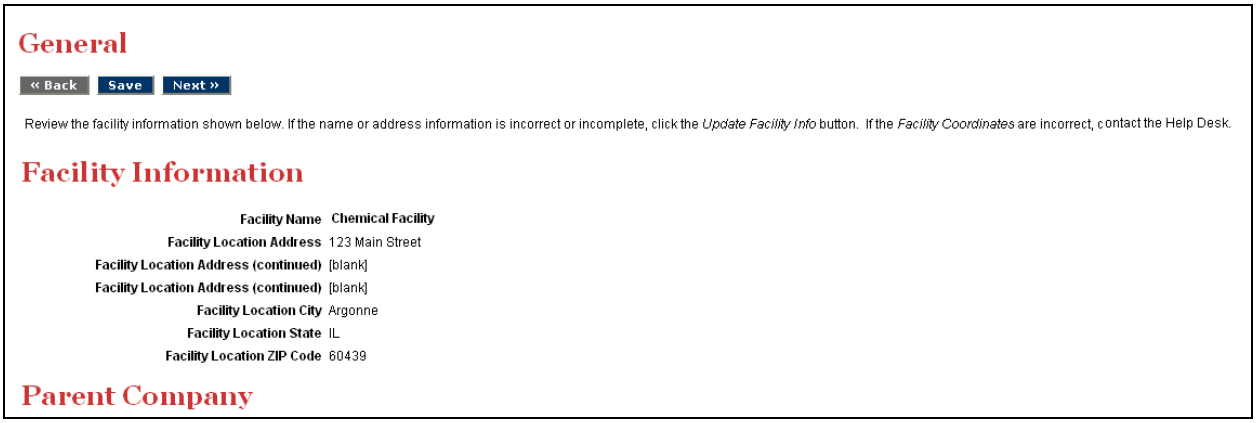

Figure 2-1 – General Facility Information

2.1 Update Facility Info

Facility Information can be entered or updated.

Facility Location Address. Update the facility's address, if needed. The address should be for its *physical* location including the street, city, state, and ZIP code (including the four-digit extension, if applicable). This address might not be the same as a facility's mailing address. Use local street and road designations, not post office or rural box numbers.

2.1.1 Parent Company Information

Parent Company Name(s) and DUNS number(s). Enter the name and DUNS number of the corporation(s) or other business entity(ies), if any, that controls at least 50 percent of the voting stock of the company that owns or operates the facility. If a facility is owned by a joint venture, enter the name and DUNS number of the first of the two major owners. If a facility does not have a parent company or is not owned or operated by a joint venture, please click *Other* and describe the facility's ownership situation.

2.1.2 Information on Co-located Entities

Choose the appropriate description of a facility's relationship to other entities, operations or businesses, if any, on its property (i.e., hosts a tenant on-site; is a tenant on another entity's facility; is the sole occupant of the property). A facility that is co-located shares a site with another company's facility through either a host or a tenant agreement. If a facility does not share a site with another facility, it is the sole tenant and you should select *Not applicable*.

If the facility is host to a co-located tenant facility or is a co-located tenant facility, please provide the name and EPA RMP facility ID for each other host/tenant facility, if applicable. Add additional rows if necessary. If the facility does not share its property with another facility, leave this field blank.

2.1.3 Security Vulnerability Assessment

Has a security vulnerability assessment been conducted for this facility? If an SVA has been conducted for this facility, provide the methodology and completion date for the most recent SVA.

2.1.4 Additional Facility Information

Facility NAICS. Provide the five- or six-digit NAICS code that corresponds most closely to the primary activity of the facility as a whole. The first three digits of the code define a major business sector (e.g., 325 represents chemical manufacturing), and the last two or three digits indicate an establishment's specialty within the major sector (e.g., 325131 represents Inorganic Dye and Pigment Manufacturing). NAICS codes are maintained by the U.S. Census Bureau and can be found on the U.S. Census Bureau website at http://www.census.gov/epcd/naics02/.

Facility DUNS. The nine-digit DUNS number is a unique identifier that allows facility information to be cross-referenced with other business information. If a facility has a DUNS number, it should be available from your financial officer or corporate headquarters. It can also be located through Dun and Bradstreet at http://www.dnb.com.

EPA RMP Facility ID. If your facility conducts EPA RMP-covered processes, fill in the unique 12-digit number assigned to the facility by the RMP Reporting Center. The RMP Reporting Center includes this number in its acknowledgment letter to the facility. If a facility does not operate an RMP-covered process, leave this field blank.

Owner Name. This may be a person, company, cooperative, state, municipality, or other entity. It may or may not be the same as the name entered for the facility operator.

Operator Name. Enter the name of the person or entity that has responsibility for the daily operations of the facility. This may be a person, company, cooperative, state, municipality, or other entity, and may or may not be the same as the name entered for the facility owner. If the owner and operator are the same, enter the same information in both data fields.

Number of Full Time Employees. Enter the number that represents the typical maximum number of employees/full-time contractors on-site at any given time. Do not include occasional times of a higher on-site workforce, such as turnarounds, in this estimate. Do not use commas when entering data.

2.1.5 Latitude and Longitude

Verify that the latitude/longitude is correct. It is a KEY piece of information and is essential in evaluating the risk level for a given facility. There are a variety of commercial websites available on the internet that you can use to verify latitude and longitude. Latitude and longitude cannot be changed from this screen; contact the Help Desk to modify incorrect latitude or longitude.

2.2 Security/Vulnerability Issues

In the CSAT Top-Screen and SVA, the facility answered a number of questions pertaining to one or more security and/or vulnerability issues. Based on the facility's responses, none, some, or all of these security/vulnerability issues may be identified in the DHS Final Notification Letter. Any security/vulnerability information from the facility's Final Notification Letter will be pre-populated here. You must confirm the accuracy of this pre-populated information. The SSP tool will allow you to demonstrate how your facility will address these security/vulnerability issue(s). Additionally, in section 2.2.2 the SSP tool allows you to identify other security/vulnerability issues and associated COI, which are not listed in the Final Notification Letter, that your facility believes to present significant security concerns.

2.2.1 Security/Vulnerability Issues From Final Notification Letter

You should review the list of security/vulnerability issues and COI and compare it to the DHS Final Notification Letter. Security/vulnerability issue(s) may include:

- Release-toxic, release-flammable, and/or release-explosive chemicals with the potential for offsite impacts;
- Theft-EXP/IEDP (explosive/improvised explosive device precursor) chemicals, theft-WME (Weapons of Mass Effect) chemicals, and theft-CW/CWP (chemical weapons/chemical weapon precursor) chemicals;
- Sabotage/contamination chemicals; and/or
- Other security/vulnerability information specified in the Final Notification Letter

If no security/vulnerability issues appear in the SSP tool at this point, please contact the Help Desk.

Is the pre-populated information listed above consistent with the information found on the facility's DHS Final Notification Letter? [Q:1.9-13848] If the security/vulnerability issues listed are correct and complete, select *Yes* to the question. If the security/vulnerability issues listed are not consistent with the facility's Final Notification Letter, select *No* to be directed to a help screen with instructions to contact the Help Desk. The facility must satisfy the applicable RBPS for the security/vulnerability issues, COI, and any other chemicals identified in its Final Notification Letter.

2.2.2 Additional Security Issues and Other COI

In this section, the SSP tool allows you to provide information about any other security/vulnerability issues of significance to your facility. This section of the SSP tool pre-populates the information from the facility's Final Notification Letter. You may then choose to provide information on additional security/vulnerability

issues and associated COI that concern the facility from a security standpoint. To do so, the tool presents you with a list of CFATS security/vulnerability issues, and related COI, to assist in identifying any security/vulnerability issues that DHS has not already identified but that your facility believes to be of concern. The information you provide in this section may be considered in DHS' evaluation of your facility's SSP.

Does the facility have security/vulnerability issues related to release-toxic COI? [Q:2.0-13720]

Does the facility have security/vulnerability issues related to release-flammable COI? [Q:2.0-13722]

Does the facility have security/vulnerability issues related to release-explosive COI? [Q:2.0-13724]

Does the facility have security/vulnerability issues related to theft-EXP/IEDP COI? [Q:2.0-13726]

Does the facility have security/vulnerability issues related to theft-WME COI? [Q:2.0-13728]

Does the facility have security/vulnerability issues related to theft-CW/CWP COI? [Q:2.0-13730]

Does the facility have security/vulnerability issues related to sabotage/contamination COI? [Q:2.0-13732]

If additional security issues are selected, you will be asked to identify the COI, if any, associated with those additional security/vulnerability issues.

If no additional security/vulnerability issues or COI are selected, you will continue to the Summary section.

2.2.3 Summary of Security/Vulnerability Information

After you have identified all of the security/vulnerability issue(s), COI, and any other chemical(s) listed in your facility's Final Notification Letter, a summary page is shown, highlighting the information provided. This list should be carefully reviewed for accuracy before continuing.

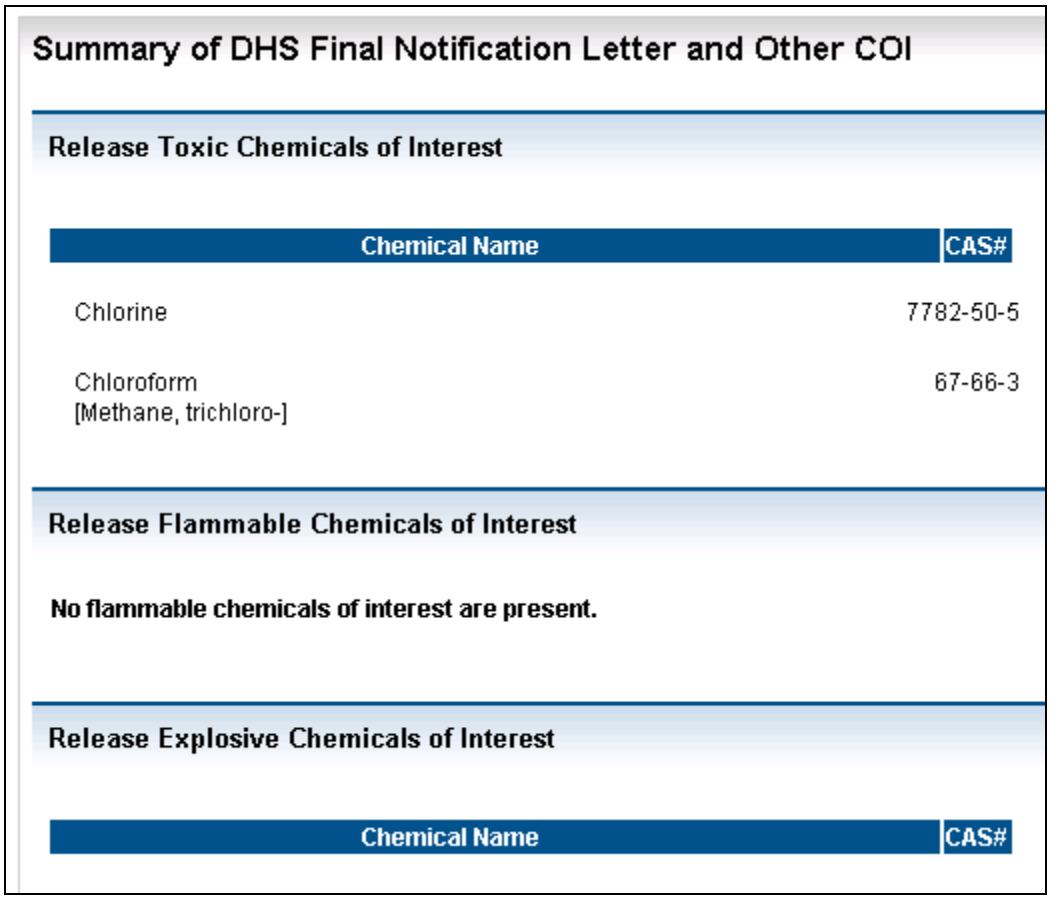

Figure 2-3 – Summary of Facility Information

Once you review the summary, you must answer *Yes* or *No* to the following question.

Have all of the COI and current security/vulnerability issues been entered? [Q:2.9-18424]

If you answer *No*, then you should return to the Facility Security Issues page of the CSAT SSP. If you answer *Yes*, then you will continue with CSAT information submission.

2.3 CSAT Submissions

Is this the initial CSAT SSP Submittal? [Q:2.95-18411]

The response format is **mm/dd/yyyy**. (e.g. May 1, 2006 is entered as 05/01/2006.)

On what date did the facility submit its most recent CSAT Top Screen? [Q:2.95-18409]

On what date did the facility submit its most recent CSAT SVA? [Q:2.95-18410]

If you indicated that this was not the initial SSP submittal, **on what date did the facility submit its most recent CSAT SSP?** [Q:2.95-18412]

Click *Next* to continue to the Facility Operations section.

3.0 Facility Operations

3.1 Facility Description

This section of the SSP tool is designed to collect information that will provide DHS with a clearer understanding of the type of facility and its surrounding environment.

What is the facility type? [Q:3.0-13871] Choose the facility type that best describes the facility. Use the drop down box to select a facility type. If no answer accurately describes the facility type, select *Other* and enter a description in the text box [Q:3.0-14051].

What is the local Office of Emergency Management (OEM)? [Q:3.0-13934] Use the drop down box to select the OEM with jurisdiction in the area where the facility is located. If the facility operates under multiple OEM authorities, enter the primary responding jurisdiction here, and then select *Other* and enter a description in the text box for additional organizations. If no answer accurately describes the facility type, select *Other* and enter a description in the text box. [Q:3.0-14052]. **Enter the name of the local jurisdiction** [Q:3.0-13935].

What is the locale setting of the facility? [Q:3.0-13936] Choose the locale setting that best describes the facility. If no answer accurately describes the setting, select *Other* and enter a description in the text box [Q:3.0-13937].

What is the construction type of the facility? [Q:3.0-14053] Choose the construction type that best describes the facility. If no answer accurately describes the construction type, select *Other* and enter a description in the text box [Q:3.0-14054].

When the Facility Description page is complete, click *Next* to move to the Facility Contact Information section.

3.2 Facility Security Information

The following questions request information about the facility's main security personnel and request information about whether the facility implements other security plans recommended by other agencies.

Provide the contact name and phone number for the individuals listed below. The phone number format is (xxx)xxx-xxxx.

Facility Security Officer [Q:3.1-13939], [Q:3.1-13940]
Assistant Facility Security Officer [Q:3.1-13941], [Q:3.1-13942]
Corporate Security Officer [Q:3.1-13943], [Q:3.1-13944]
Cyber Security Officer [Q:3.1-13945], [Q:3.1-13946]

Does the facility implement security plans required or recommended by the following agencies? [Q:3.1-18675] Select *Yes* or *No*, as appropriate, for each of the listed agencies. If the facility implements

security plans/procedures required or recommended by any agency or agencies not listed here, select *Other* and then describe that agency or those agencies in the *Other* box. [Q:3.1-18676]

3.3 On-site Emergency Response Capabilities

This section of the SSP tool provides the facility with the opportunity to submit information related to any existing on-site emergency response capabilities.

Does the facility have a fire department? [Q:3.9-18433] Select *Yes* or *No*.
Does the facility have a HAZMAT team? [Q:3.9-18434] Select *Yes* or *No*.
Does the facility share any of its emergency response capabilities with other facilities or entities? [Q:3.9-18435] Select *Yes* or *No*.
Does the facility have an emergency management team available? [Q:3.9-18436] Select *Yes* or *No*.
Does the facility have any Special Response Capabilities? [Q:3.9-18437] Select *Yes* or *No*.

For any *Yes* responses, more detailed questions will be presented. If all responses are *No*, the SSP tool will direct you to the Emergency Management Information section.

3.3.1 On-site Emergency Response Capabilities

Identify the other facilities or entities with which this facility shares emergency response capabilities. [Q:3.91-18442] For each entry, type the name in the text box and click *Add*. A new box will appear. Add all other facilities or entities in the additional text boxes.

E**nter the number of on-site emergency management team members.** [Q:3.91-18444]
Choose the special response capability available on-site. Select all capabilities that apply. [Q:3.91-18445] Use the radio buttons to select all the response capabilities available on-site.

3.4 Emergency Management Information

The following sections of the SSP tool collect information on the facility's local emergency management resources. The facility is responsible for obtaining as much of this information as possible. The Department recognizes that the answers to the following questions may vary by day or time. Therefore, where applicable, average response times are acceptable responses to these questions.

Is the facility able to shelter-in-place? [Q:4.0-18738] Select *Yes* or *No*.
Does the facility have a community notification system? [Q:4.0-18749] Select *Yes* or *No*.

3.4.1 Police Information

N**ame of the local police jurisdiction** [Q:4.0-13949] and **phone number** [Q:4.0-13950]. The phone number format is (xxx)xxx-xxxx.

Number of full-time police officers [Q:4.0-13951] Select *Yes*, *No*, or *Unknown*.
Local police SWAT team available? Q:4.0-13952] Select *Yes*, *No*, or *Unknown*.

Local police bomb squad available? [Q:4.0-13953] Select *Yes*, *No*, or *Unknown*.
Local police HAZMAT team available? [Q:4.0-13954] Select *Yes*, *No*, or *Unknown*
Local police Emergency Management Capabilities available? [Q:4.0-17899] Select *Yes*, *No*, or *Unknown*

Distance to nearest police station (miles) [Q:4.0-13955] Round distance up to nearest tenth of a mile. (For example, for 0.25 miles enter 0.3 miles)
Time for first response officer to reach facility (average) [Q:4.0-13957] Use the drop down box to select the average number of minutes.
Minimum time needed for police to mount tactical response [Q:4.0-13959] Use the drop down box to select the number of minutes, if known.
Was tactical response time tested? [Q:4.0-13960] Select *Yes* or *No*. If *Yes*, then complete the **date of tactical response test** [Q:4.0-13961].

Does the police department conduct response tests outside of a facility drill or exercise? [Q:4.0-18750] Select *Yes*, *No* or *Unknown*.

3.4.2 Fire Department Information

Number of full-time on-site fire fighters [Q:4.1-19181]
On-site fire department foam truck available? [Q:4.1-19182] Select *Yes*, *No*, or *Unknown*.
On-site fire department HAZMAT team available? [Q:4.1-19183] Select *Yes*, *No*, or *Unknown*.
On-site fire department EMT available? [Q:4.1-19184] Select *Yes*, *No*, or *Unknown*.

Name of the local fire jurisdiction [Q:4.1-13968] and **phone number** [Q:4.1-13969]. The phone number format is (xxx)xxx-xxxx.

Number of full-time fire fighters [Q:4.1-13970]
Local fire department foam truck available? [Q:4.1-13972] Select *Yes*, *No*, or *Unknown*.
Local fire department HAZMAT team available? [Q:4.1-13973] Select *Yes*, *No*, or *Unknown*.
Local fire department EMT available? [Q:4.1-13971] Select *Yes*, *No*, or *Unknown*.

Distance to nearest fire dept. station (miles) [Q:4.1-13974] Round distance up to nearest tenth of a mile. (For example, for 0.25 miles, enter 0.3 miles).
Time for first response apparatus to reach facility (average) [Q:4.1-13975] Use the drop down box to select the average number of minutes.
Minimum time needed for fire department to set up and respond once on-site at the facility [Q:4.1-13976] Use the drop down box to select the number of minutes.
Was the response time tested? [Q:4.1-13977] Select *Yes* or *No*. If *Yes*, then complete the date of **response test** [Q:4.1-13978].

3.4.3 Emergency Management Team (EMT) Information

The questions in this section collect information related to emergency medical response capabilities. The term EMT is used in these questions to mean Emergency Medical Technician but can also mean paramedics or other emergency medical personnel.

Number of full-time EMT staff on-site [Q:4.2-19185]

On-site EMT life support unit available? [Q:4.2-19186] Select *Yes*, *No*, or *Unknown*.
On-site EMT water rescue available? [Q:4.2-19187] Select *Yes*, *No*, or *Unknown*.
On-site EMT HAZMAT team available? [Q:4.2-19188] Select *Yes*, *No*, or *Unknown*.

Name of the local EMT jurisdiction [Q:4.2-13979] and **phone number** [Q:4.2-13980]. The phone number format is (xxx)xxx-xxxx.

Number of full-time EMT staff [Q:4.2-13981]
Local EMT life support unit available? [Q:4.2-13982] Select *Yes*, *No*, or *Unknown*.
Local EMT water rescue available? [Q:4.2-13983] Select *Yes*, *No*, or *Unknown*.
Local EMT HAZMAT team available? [Q:4.2-13984] Select *Yes*, *No*, or *Unknown*.

Distance to nearest Trauma Center (miles) [Q:4.2-13985] Round distance up to nearest tenth of a mile. (For example, for 0.25 miles, enter 0.3 miles)
Time for first response EMT to reach facility (average) [Q:4.2-13986] Use the drop down box to select the average number of minutes.
Minimum time needed to transport casualties to Trauma Center [Q:4.2-13987] Use the drop down box to select the number of minutes.
Was the response time tested? [Q:4.2-13988] Select *Yes* or *No*. If *Yes*, then complete the **date of response test** [Q:4.2-13989]

3.4.4 Local Mutual Assistance Groups (MAG)

Enter a MAG name, if any, and click the *Add* button. A new box will appear for additional MAGs. Continue adding MAGs until all applicable groups have been provided. Then click *Describe* for each MAG and provide the requested information.

If the facility is not a member of a MAG, answer *Yes* to question number [Q:4.3-17722] and continue to the next section on Special Response Capability.

Short description of the local mutual assistance group [Q:4.31-13990] and **phone number** [Q:4.31-13991]. The phone number format is (xxx)xxx-xxxx.
How many groups/facilities are included in the MAG? [Q:4.31-18839]

Number of MAG member companies [Q:4.31-13994]

Time for capable response to reach facility (average) [Q:4.31-13999] Use the drop down box to select the average number of minutes.
Does the facility conduct drills or exercises to include the MAG? [Q:4.31-18840] Select *Yes* or *No*.
Minimum time needed for MAG to begin on-scene response [Q:4.31-14000] Use the drop down box to select the number of minutes.
Was the response time tested? [Q:4.31-14001] Select *Yes* or *No*. If *Yes*, then complete the **date of response test** [Q:4.31-14002]

When all MAG information has been entered and completed, answer *Yes* to question number **[Q:4.3-17722]** and continue to the Special Response Capability section.

3.5 Special Response Capability

This section of the SSP tool collects information on special response capabilities around high-risk facilities. The facility may provide information about Special Response Capabilities whether of not there is currently an agreement or expectation that the specific capability will respond in the event of a relevant chemical security incident. In this section, you should list any capabilities not already included in the previous sections on police, fire and emergency management technician. For example, a military base or hostage negotiation team in the facility's community should be noted here.

Are other special response capabilities available? [Q:4.4-14030] Select *Yes*, *No* or *Unknown*. If the answer is *Yes*, list the agencies with special response capabilities below.

Responding Agency [Q:4.4-14031] Enter a responding agency name and click the *Add* button. A new box will appear for additional agencies. Continue adding agencies until all applicable agencies have been provided. Then click *Describe* for each agency and provide the requested information.

What is the government level? [Q:4.41-14056] Use the drop down box to select the government level of the responding agency. If *Other* is selected, enter a description [Q:4.41-14067]

What is the distance from the responding agency (miles)? [Q:4.41-14057] Round distance from the facility to the responding agency up to nearest tenth of a mile. (For example, for 0.25 miles, enter 0.3 miles.)

What is the average arrival time for the response? [Q:4.41-14058] Use the drop down box to select the average time in minutes.

Is there a formal, written agreement with the responding agency? [Q:4.41-14060] Select *Yes* or *No*.

Choose the special response capability. Select all capabilities that apply. [Q:4.41-14059]

Click *Next* to return to the Capabilities Section.

Are there special response capabilities available not included in the list? [Q:4.4-14037] If there are other types of special response capabilities not included in the drop-down list, select *Yes* to describe the other capabilities on the next page.

3.5.1 Other Response Agencies with Special Capabilities Not Included in the Previous List

Other Response Agencies with Special Capabilities Not Included in The Previous List [Q:4.5-14038] Enter a responding agency name and click the *Add* button. A new box will appear for additional agencies. Continue adding agencies until all applicable agencies have been provided. Then click *Describe* for each agency and provide the requested information.

What is the government level? [Q:4.51-14062] Use the drop down box to select the government level of the responding agency. If *Other* is selected, enter a description [Q:4.51-14069]

What is the distance from the responding agency (miles)? [Q:4.51-14063] Round distance from the facility to the responding agency up to nearest tenth of a mile. (For example, for 0.25 miles, enter 0.3 miles.)

What is the average arrival time for the response? [Q:4.51-14064] Use the drop down box to select the average time in minutes.

Is there a formal, written agreement with the responding agency? [Q:4.51-14066] Select *Yes* or *No*.

Choose the special response capability. Select all capabilities that apply. [Q:4.51-14065]

Click *Next* to return to the Other Capabilities Section.

When all special response agencies have been entered, answer *Yes* to the question: **Have all other special response capabilities been entered?** [Q:4.5-14044]

3.6 Facility Personnel Staffing

The following questions in the SSP tool are related to the facility's employee staffing. For each question, provide the current number of employees for each category.

Enter the Number of Employees.

What number are full-time? [Q:4.6-14076]
What number are part-time? [Q:4.6-14077]
What number typically are contractors? [Q:4.6-14078]
What number are other types? [Q:4.6-14079] The facility should include any other types of employees or other facility personnel (such as interns, seasonal workers, or volunteers) not accounted for in the prior questions.

Enter the Number of Security Officers.

What number are full-time? [Q:4.6-14080]
What number are part-time? [Q:4.6-14081]
What number typically are contractors? [Q:4.6-14082]
What number are other types? [Q:4.6-14083] The facility should include any other types of security officers (such as interns or volunteers) not accounted for in the prior questions.

3.7 Facility Work-force Staffing

Provide a name or short description for each work shift or period. Add as many work shifts as necessary to account for different starting/ending times and numbers of employees present. Click the *Add* button to add a **work shift** [Q:4.8-18510] and then use the *Describe* button to answer the detailed questions.

For each day of the week, enter the **starting and ending time of day of facility operations** [Q:4.81-18512], [Q:4.81-18513], [Q:4.81-18514], [Q:4.81-18515], [Q:4.81-18516]
Enter the **number of employees** present during each period.

If a work shift does not apply on a particular day, enter *NA* for the times and 0 for the number of employees.

Click *Next* to return to the Workforce Operations Section.

Have all the work shifts been entered? [Q:4.8-18511] When all work shifts have been described, answer *Yes* to this question.

3.8 Chemical Operations

The following questions cover the facility's chemical operations. When answering these questions, you should only answer with respect to the COI and any other chemicals included in the summary described in Section 2.2.3. This section combines the information on security/vulnerability issues and COI identified in the DHS Final Notification Letter with any information the facility chooses to provide about other security/vulnerability issues that raise security/vulnerability issues.

Does the facility ship COI? [Q:5.0-14120] Select *Yes* or *No*.
Does the facility ship other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18466] Select *Yes* or *No*.
Does the facility sell COI? [Q:5.0-14121] Select *Yes* or *No*.
Does the facility sell other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18467] Select *Yes* or *No*.
Does the facility receive COI? [Q:5.0-14119] Select *Yes* or *No*.
Does the facility receive other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18468] Select *Yes* or *No*.
Does the facility manufacture COI? [Q:5.0-18586] Select *Yes* or *No*.
Does the facility manufacture other chemicals identified on the facility's DHS Final Notification Letter? [Q:5.0-18587] Select *Yes* or *No*.

If the facility answers *Yes* to manufacturing, shipping, selling, and/or receiving any COI, answer the additional questions described in Section 3.8.1 below. If the facility does not ship, sell, receive and/or manufacture any COI, continue to Section 3.9 (ASPs).

3.8.1 COI - Chemical Operations – cont'd

Chemicals of Interest Shipments

For each of the listed COI or other chemicals listed on the facility's DHS Final Notification Letter, indicate the shipping method by clicking the appropriate *Yes*/*No* radio button.

By Truck [Q:5.1-14203, 5.1-14208, 5.1-14213, 5.1-14218, 5.1-14223, 5.1-14228, 5.1-14233, 5.1-22365],
By Rail [Q:5.1-14204,5.1-14209, 5.1-14214, 5.1-14219, 5.1-14224, 5.1-14229, 5.1-14234, 5.1-22367],
By Barge [Q:5.1-14205,5.1-14210, 5.1-14215, 5.1-14220, 5.1-14225, 5.1-14230, 5.1-14235, 5.1-22366],
By Pipeline [Q:5.1-18917, 5.1-18919, 5.1-18920, 5.1-18921, 5.1-18922, 5.1-18923, 5.1-18924, 5.1-22368]

For other shipping methods, enter the method in the **By Other Method** text box [Q:5.1-14206, 5.1-14211, 5.1-14216, 5.1-14221, 5.1-14226, 5.1-14231, 5.1-14236, 5.1-22369].

Chemicals of Interest Sales

Indicate whether any of the listed COI or any other chemicals listed on the facility's DHS Final Notification Letter are sold by the facility by clicking the appropriate *Yes/No* radio buttons [Q:5.2-14245, 5.2-14247, 5.2-14249, 5.2-14251, 5.2-14253, 5.2-14255, 5.2-14257, 5.2-22489].

Select All Industries that the Facility Supplies [Q:5.2-14258] Use the radio buttons to select all the types of industrial clients that apply. If needed, select *Other* and enter other client industries in the *Other* text box [Q:5.2-14259].

Chemicals of Interest Received

For each of the listed COI or other chemicals listed on the facility's DHS Final Notification Letter, indicate the appropriate receiving method by clicking the appropriate *Yes/No* radio button.

By Truck [Q:5.3-14152, 5.3-14171, 5.3-14175, 5.3-14179, 5.3-14183, 5.3-14187, 5.3-14191, 5.3-22490],
By Rail [Q:5.3-14153, 5.3-14172, 5.3-14176, 5.3-14180, 5.3-14184, 5.3-14188, 5.3-14192, 5.3-22491],
By Barge [Q:5.3-1415,5.3-14173, 5.3-14177, 5.3-14181, 5.3-14185, 5.3-14189, 5.3-14193, 5.3-22492],
By Pipeline [Q:5.3-22496, 5.3-22497, 5.3-22499, 5.3-22500, 5.3-22501, 5.3-22502, 5.3-22503, 5.3-22493]
For other receiving methods, enter it in the **By Other Method** text box [Q:5.3-14566, 5.3-14174, 5.3-14178, 5.3-14182, 5.3-14186, 5.3-14190, 5.3-14194].

Chemicals of Interest Manufactured

Indicate whether any of the listed COI or any other chemicals listed on the facility's DHS Final Notification Letter are manufactured by the facility by clicking the appropriate *Yes/No* radio buttons [Q:5.4-18598, 5.4-18603, 5.4-18608, 5.4-18613, 5.4-18618, 5.4-18623, 5.4-18628, 5.4-22495].

3.9 Alternative Security Program

CFATS provides all high-risk facilities with the option of submitting an ASP in place of the SSP. DHS may approve an ASP in whole or in part, or subject to revisions or supplements, if the ASP meets the requirements of 6 CFR § 27.225. If a facility elects to submit an ASP rather than submit the CSAT SSP, this section describes the process for uploading the relevant ASP files into the CSAT SSP tool. Before deciding whether to proceed with that option, a high-risk facility should be familiar with the requirements of 6 CFR § 27.225.

Alternative Security Program [Q:5.6-17939] **Do you want to upload an ASP in lieu of using the CSAT SSP?** If the user plans to upload an ASP and not complete the CSAT SSP, answer *Yes*, and follow the remaining instructions. If the user does not plan to upload an ASP, select *No*, and the user will be prompted to continue the CSAT SSP.

3.9.1 ASP Documents

Before uploading an ASP, the user will be asked questions related to the factors (see 6 CFR §§ 27.225, 27.235) for submitting an ASP in lieu of an SSP and otherwise related to the Department's determination of whether to approve an ASP.

Does the ASP address each security/vulnerability issue identified in the facility's SVA, and identify and describe security measures to address each such security/vulnerability issue? [Q:5.61-18413] Select *Yes* if the ASP addresses each security/vulnerability issue and identifies and describes the security measures addressing each security/vulnerability issue.

Does the ASP identify and describe how security measures selected by the facility will address the risk-based performance standards and potential mode of terrorist attack? [Q:5.61-18414] Select *Yes* if the ASP identifies and describes how the security measures address the risk-based performance standards and potential mode of terrorist attack.

Does the ASP identify and describe how security measures selected and utilized by the facility will address each applicable performance standard for the appropriate risk-based tier for the facility? [Q:5.61-18415] Select *Yes* if the ASP identifies and describes how the security measures will meet the applicable performance standard for the appropriate risk-based tier.

Does the ASP provide other information that the Assistant Secretary has deemed necessary, through the DHS Final Notification Letter or other means, regarding facility security? [Q:5.61-18416] Select *Yes* if the ASP specifies other information deemed necessary by the Assistant Secretary regarding chemical facility security.

If you answer *Yes* to all of these questions, you will continue with the ASP uploading procedure. If you answer *No* to any of these questions, you will be provided with the following question: [Q:5.62-18453] **The ASP does not address all pertinent factors in 6 CFR 27. Do you wish to continue to upload an ASP in lieu of the CSAT SSP?** By selecting the *Yes* radio button, you will continue with the ASP questions and the ASP uploading procedure. By selecting the *No* radio button, you will return to entering information into the CSAT SSP starting at Section 3.10 of this document.

3.9.2 Upload ASP Documents

Each facility that elects to continue uploading an ASP after answering the questions described in the previous section shall continue on to this section to answer additional ASP questions and to upload the ASP itself.

If facility did submit a non-CSAT SVA, what is the date of that submittal? [Q:5.7-18182] The response format is mm/dd/yyyy.

To upload the ASP files, enter each file name and click the *Add* button. The application will then provide a button for detailed information. Click the *Describe* button and then browse to select a file on your computer or network to submit. Upload all documents associated with the ASP.

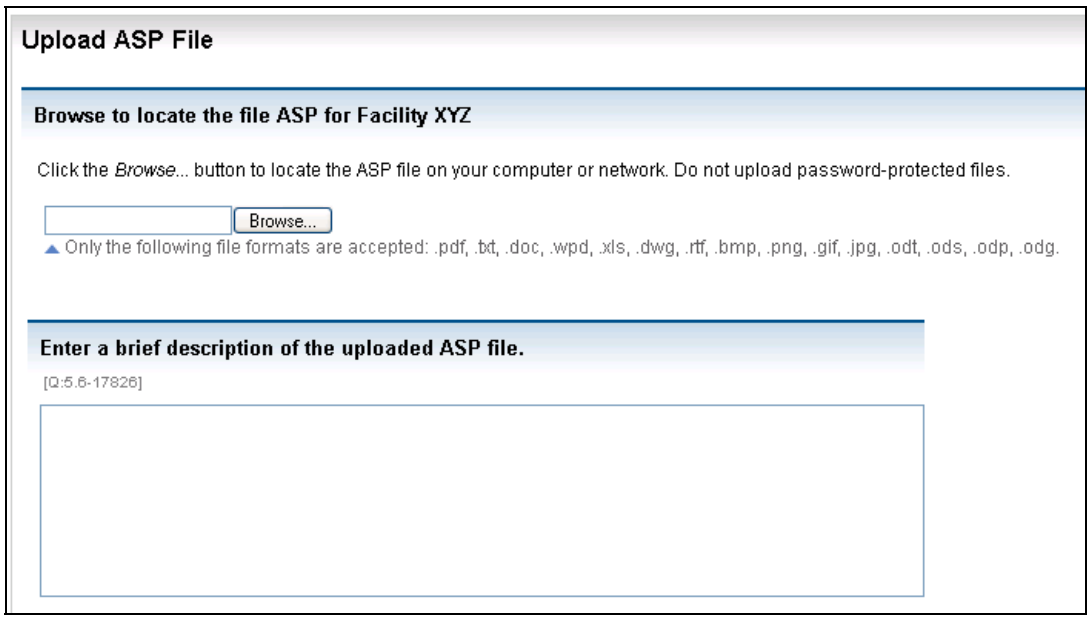

Figure 3-1 – ASP Upload Screen

When all ASP documents have been uploaded, answer *Yes* to the question asking if all the documents have been provided: **Have you uploaded all ASP documents and provided detailed ASP information in your uploads?** [Q:5.7-17819].

3.9.3 ASP Submission

If you have answered the above questions and uploaded an ASP in lieu of an SSP, as instructed, you have completed your use of the CSAT SSP tool. The CSAT system will upload this information to DHS, and DHS will contact your facility with the results of its review of the facility's ASP, and with the next steps, if any, under CFATS.

3.9.4 ASP Completion

Instructions on final validation, including validation of the fact that the facility submitted an ASP, and instructions on final submission are detailed in Section 6.

3.10 Upload Facility Schematics

The SSP Tool provides the facility with the ability to upload a facility schematic. The facility schematic could include the locations of main site features, could show a facility's assets (as defined in Section 5 of these SSP instructions), and could show security features such as perimeter fencing. There could be more than one facility schematic (i.e., an overall facility site map followed by more detailed maps that show groups of buildings, process areas, storage areas, etc.) that a facility would like to share with DHS. The schematic(s) should be current and reflect the existing operations at the facility.

Facility Schematics Upload [Q:5.9-22809] **Do you want to upload facility schematics or photographs that support the SSP?** If the facility plans to upload a schematic, answer *Yes*, and follow the remaining instructions. If the facility does not plan to upload a schematic, select *No*, and the facility will be prompted to continue the CSAT SSP.

3.9.5 Upload Facility Schematics and Photographs

For a facility that elects to upload facility schematics and photograph files, enter each file name [Q:5.81-22818] and click the *Add* button. The application will then provide a button for detailed information. The user will click the *Describe* button and then browse to select a file on his/her computer or network to submit. Upload all documents associated with the schematic(s) and/or photograph(s).

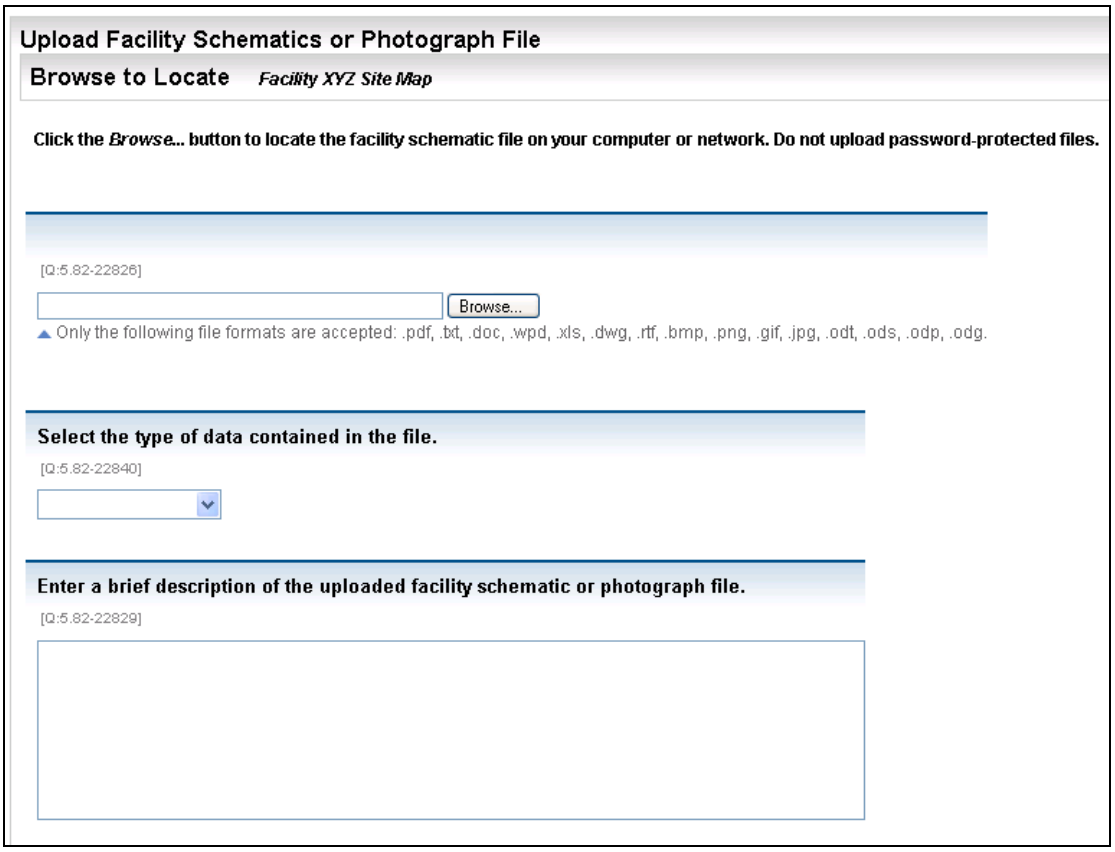

Figure 3-2 – Facility Schematic(s) Upload Screen

When all files have been uploaded, answer *Yes* to **Have you uploaded all the facility schematic files and provided detail information?** [Q:5.81-22819], and the facility will be prompted to continue the CSAT SSP.

4.0 Facility Security

DHS recognizes that a facility typically administers most security measures on a facility-wide basis. However, facilities also often customize security for certain assets within a facility. The SSP tool enables a facility to describe both its facility-wide security, as well as security measures unique to particular assets, such as cyber systems, raw material warehouses, or research and development laboratories.

In this section, the facility will describe its existing and – if the facility so chooses - its planned and proposed facility-wide security measures. Where security is administered uniformly across a facility and its assets, a facility need only address the RBPS at the facility level. In that case, the information provided about the facility-wide security measures is understood to cover all of the facility's assets.

However, a facility that administers some of its security on a facility-wide basis, but also has specialized security to protect certain assets that are relevant to satisfying certain RBPS (e.g., cyber systems) must also address those RBPS on an asset-specific basis by naming, describing and distinguishing the asset-specific security measures. This approach is explained in Section 5.0, the Asset Security section, of these instructions.

For more detailed discussion of how the terms 'facility' and 'assets' are related to the RBPS, refer to DHS' Risk-Based Performance Standards Guidance, which will be available at http://www.dhs.gov/chemicalsecurity. While a facility can always be identified by a geographical location (latitude and longitude), in some cases, facilities may include assets, such as a cyber-security system, outside the physical boundary of the facility.

4.1.1 Addressing RBPS

Each high-risk facility that receives a final tier designation must select, develop in its SSP, and implement appropriate risk-based measures designed to satisfy the RBPS established in 6 CFR §27.230. In this section each facility must address every RBPS by indicating whether or not it implements or – if the facility so chooses - plans to implement security measures for that RBPS. However, not all facilities will need to implement security measures for every RBPS. Rather, a facility must have security measures satisfying those RBPS that DHS determines apply to the facility. Failure to provide information about security measures relevant to a given RBPS may result in the need to submit a revised SSP and, in some cases, ultimately could lead to disapproval of a facility's SSP.

DHS expects certain RBPS typically to be applicable to virtually every facility, at least at the facility-wide level. These RBPS include:

RBPS 1 - Restrict Area Perimeter;
RBPS 3 - Screen and Control Assets;
RBPS 4 - Deter, Detect, and Delay;
RBPS 5 - Shipping, Receipt, and Storage;
RBPS 8 - Cyber Security;
RBPS 9 - Response;

RBPS 10 - Monitoring;
RBPS 11 - Training;
RBPS 12 - Personnel Surety;
RBPS 13 - Elevated Threats;
RBPS 14 - Specific Threats, Vulnerabilities, or Risks;
RBPS 15 - Reporting of Significant Security Incidents;
RBPS 16 - Significant Security Incidents and Suspicious Activities;
RBPS 17 - Officials and Organization; and
RBPS 18 - Records.

DHS expects that RBPS 2 (Secure Site Assets) typically will be applicable to all facilities at either the facility-wide level or the asset level (or both). However, a facility must address RBPS 2 for each asset whether or not facility-wide security measures were previously entered. A facility will describe any asset-specific security measures in Section 5.

DHS also expects that the following RBPS typically will be applicable only to facilities that have certain security/vulnerability issues:

RBPS 6 - Theft and Diversion; and
RBPS 7 - Sabotage.

For facilities that have a Theft-Diversion and/or Sabotage security/vulnerability issue(s), the user will have the option in the SSP tool to address RBPS 6 and/or 7 at the facility-wide or asset level (or both).

Addressing Individual RBPS and Entering Security Measures

To start addressing the RBPS, click each RBPS box in turn, as shown in Figure 4-2, and answer *Yes* or *No* as to whether or not the facility has existing, planned or proposed security measures for that RBPS. If the facility selects *No*, the facility has addressed the RBPS but has indicated that it has no security measures for satisfying that RBPS, if applicable. The facility will then be directed to the next RBPS.

Figure 4-2 – RBPS Questions

If the facility selects *Yes* for any RBPS, the SSP tool will then direct the facility to enter its facility-wide security measures for that RBPS. The facility should select the security measures that most accurately and completely describe its ***existing*** facility-wide security measures. Where the facility believes the security measures provided by the SSP tool do not accurately or completely depict its security measure, the facility should select *Yes* for *Other* and describe/explain this security feature in the *Other* text box provided.

For RBPS 2, 3, 5, 6, and, 7 only, the facility will be asked two additional questions; does the facility have facility-wide security measures for this RBPS, and does the facility also have asset-specific security measures for this RBPS that are different from the facility-wide security measures.

4.1.2 Planned and Proposed Security Measures

At the end of each RBPS section, the facility is able to provide information on any Planned and/or Proposed security measures relative to the facility and/or its asset(s). A planned security measure may be considered by DHS in determining whether an SSP satisfies an applicable RBPS, for example, if the measure:

- Is in the process of being installed; or
- Is in the design phase but has an approved and documented capital budget; or
- Is in the bid process and has been placed for bid or bids have been received and are under review; or
- Is in a pilot phase or is in execution as a demonstration project, and has some sort of documented implementation budget and schedule.

If a facility chooses to provide information about a planned security measure for consideration, DHS may subsequently ask the facility to produce documentation confirming the planned measure. While planned measures are considered in the SSP approval process, a proposed measure is one that is under consideration by the facility but is not yet a planned measure, and will not be considered by DHS in determining whether to approve an SSP.

Proposed Measures

A facility can provide three types of information using this section of the SSP tool: 1) Proposed Security Measures the facility wants to share with DHS; 2) Existing Security Measures the facility is proposing to eliminate or remove; and 3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

Entering Proposed Security Measures

If a facility chooses to share its proposed security measures with DHS, then the facility should enter a description of the proposed security measure. The facility should label each proposed security measure using "Proposed Security Measure X" where the X would be a number for the Proposed Security Measure. A sample entry for a Proposed Security Measures could be: "Proposed Security Measure 1 – Install new 8 feet high chain link fence with one (1) foot high barbed wire topping; Proposed Security Measure 2 – Install 2 CCTV cameras at the facility's main gate." The facility can provide as much detail as necessary to convey each Proposed Security Measure to DHS.

Entering Proposals to Eliminate Security Measures

Facilities are required to list and/or describe existing security measures as part of Section 4 of their CSAT SSP submissions. Existing security measures which each covered facility describes or lists in its CSAT SSP submission may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. However, this section of the CSAT SSP tool will provide facilities the opportunity to disclose that

certain existing security measures are proposed to be removed or eliminated in the future. Of course, if a facility chooses to eliminate an existing security measure that is relevant to one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

If a facility chooses to share its proposals to eliminate security measures with DHS, then the facility should enter a description of the proposed security measure that will be eliminated and include a timeframe for when that security measure will be eliminated. The facility should label each proposed security measure to be eliminated using "Proposed Elimination X" where the X would be a number for the proposed security measure to be eliminated. A sample entry could be: "Proposed Elimination 1 – Remove existing chain link fence by September 2012; Proposed Elimination 2 – Remove 2 CCTV cameras from the facility's main gate by December 2015." The facility can provide as much detail to DHS as necessary to convey each proposed security measure to be eliminated.

Entering Proposals for Specific Security Measures Not to be Included in SSP

The SSP tool asks facilities to list and/or describe existing security measures as part of Section 4 of their CSAT SSP submissions. Existing and planned security measures which each covered facility describes or lists in its CSAT SSP submission may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. However, this section of the CSAT SSP tool will provide facilities the opportunity to propose that certain existing and/or planned security measures identified in this tool not be considered by DHS in evaluating its SSP for approval. Of course, if a facility chooses not to include an existing or planned measure that is relevant to satisfaction of one or more CFATS RBPS in its SSP, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

If a facility would like to identify existing or planned security measures in the CSAT SSP tool for a specific RBPS, but does not want DHS to consider those measures during its evaluation of the facility's SSP, the facility should make a note of the question numbers that correspond to those particular security measures. The facility should use this text box to enter a description of the security measures the facility does not want DHS to consider. The facility should label each security measure not to be included by using "Security Measure Not to be Included in SSP X [Q:#.#-#####]" where the X would be a number for the specific security measure not to be included and [Q:#.#-#####] is the question number found in the SSP tool that is related to the specific security measure not to be included. A sample entry could be, "Security Measure Not to be Included in SSP 1 – [Q:7.01-14429] Facility does not want its perimeter fence considered by DHS during evaluation of its SSP; Security Measure Not to be Included in SSP 2 – [Q:7.03-14443] Facility does not want its clear zone considered by DHS during evaluation of its SSP.

4.2 Completing Facility-wide RBPS

When the facility has addressed all RBPS and entered its related security measures by RBPS, choose *Yes* for the question **Have all Risk-based Performance Standards at the facility level been addressed and security measures entered?** [Q:6.6-14422] Answering *Yes* will take the user to the asset level security measures section described in Section 5 below.

5.0 Asset Security Measures

The Assets section is for the facility to identify and describe customized security measures provided for specific assets.

A facility should complete this section if it has identified an asset or assets for special security treatment relevant to satisfying an RBPS and did not provide information about all relevant security measures for that RBPS in the facility-wide section. The security measures unique to an asset in this section should be clearly distinguishable from facility-wide security measures. However, a facility that provided information about all its relevant security measures at the facility-wide level may rely on its facility-wide security measures and need not identify any assets or asset-specific measures in this section.

A facility should begin this section by indicating whether it is identifying any assets, as described in section 5.1 below. A facility with no assets to identify or describe should leave the **Asset Name** [Q. 26.1-14664] blank and answer *Yes* to the question **Have all assets been listed and details provided? [Q: 26.1-14665]** The user is then directed to confirm its completion of the SSP. Refer to Section 6 for instructions on submitting the SSP.

5.1 Identification of Assets

This portion of the tool recognizes that a facility may administer certain aspects of security at the facility level (e.g., personnel surety) while also applying distinct security measures to specific assets within a facility (e.g., shipping, receipt and storage area). For instance, a building where COI is packaged may be monitored with specialized surveillance equipment. This asset-specific approach to security is distinct from the facility-wide security. Given the prevalence of specialized security at chemical facilities, this section enables a facility to describe asset-specific security measures, as needed. The SSP tool is designed to provide DHS with a complete picture of a facility, as well as any asset level security measures and how the facility, and asset-specific security measures (if any) function to satisfy the RBPS.

For more detailed discussion of how the terms "facility", "assets", and "critical assets" are related to RBPS, refer to DHS' Risk-Based Performance Standards Guidance, which will be available at http://www.dhs.gov/chemicalsecurity. For example, a facility may provide information on security measures related to assets, such as:

(1) Physical security infrastructure, procedures, personnel or measures that comprise all or part of the facility's system for managing security risks.
(2) Physical safety infrastructure, procedures, personnel or measures that comprise all or part of the facility's system for managing process safety and emergency response measures,
(3) Cyber systems involved in the management of processes, process safety, security, product or material stewardship, or business management and control
(4) Vessels, process equipment, piping, transport vessels or any container or equipment used in the processing or holding of chemicals
(5) Onsite and off-site response protocols,
(6) Warehouses, vaults, storage bays, and similar infrastructure,
(7) Specially-trained, qualified personnel who are engaged in the management of security and safety risk.

In this section, the facility is to provide answers only for ***existing*** security measures at the facility.

5.1.1 Describing Assets

Begin the Asset Security Measures section by naming each asset. The asset name should be distinct enough to track over subsequent screens. This field can be up to 34 characters in length.

Click the *Add* button after entering each asset name. A new entry line will appear for additional assets. Continue adding entries until all applicable assets have been provided. Then click *Describe* for each asset and provide the requested information.

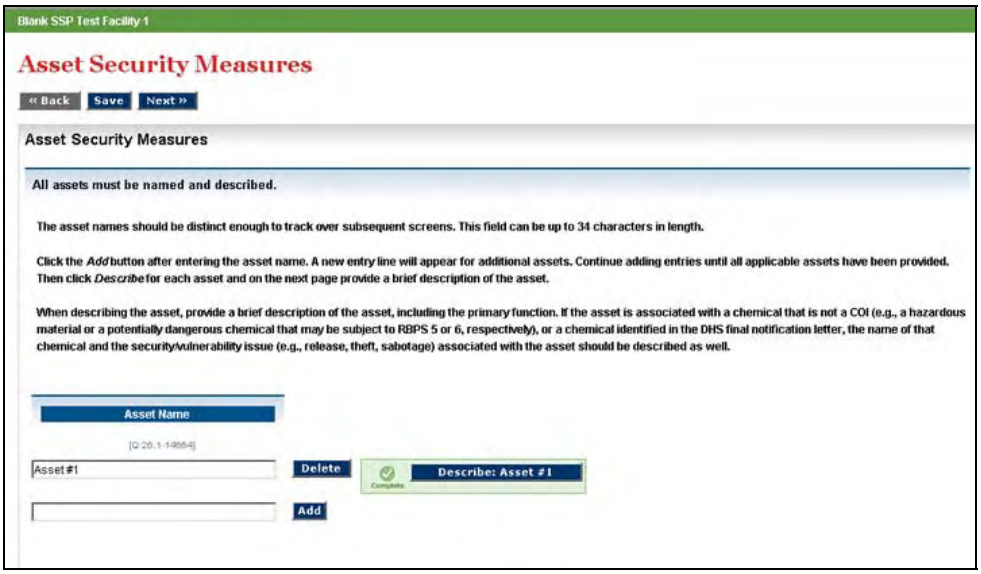

Figure 5-1 – Asset Security Measures

Describe Asset [Q:26.2-14666] Provide a brief description of the asset, including the primary function. If the asset is associated with a chemical (e.g., a hazardous material or a potentially dangerous chemical that may be subject to RBPS 5 or 6, respectively) that is not a COI or a chemical identified in the DHS final notification letter, the name of that chemical and the security/vulnerability issue (e.g., release, theft, sabotage) associated with the asset should be provided here.

Is this a critical asset? [Q:26.2-22738] For more detailed discussion of how the term "critical asset" is related to the RBPS, refer to DHS' Risk-Based Performance Standards Guidance, which will be available at http://www.dhs.gov/chemicalsecurity.

Is a COI or other chemical from the DHS final notification letter associated with this asset? [Q:26.2-17940] If the asset is related to a COI, answer *Yes*. If the asset is not related to a COI, answer *No*. If the answer is *No*, the facility must also answer *No* to all of the security/vulnerability issues listed below, and will then be directed to the next series of questions related to the RBPS.

Select All Security/Vulnerability Issues associated with this Asset. [Q:26.2-14668, 26.2-14669, 26.2-14670, 26.2-14671, 26.2-14673, 26.2-14674, 26.2-18554] Using the list of security/vulnerability

issues provided on the screen, select the ones associated with the asset. Then select any COI listed that are associated with the asset.

5.1.2 RBPS Questions

The facility will be presented with a list of the RBPS for which it indicated it had asset-specific security measures that are different from the facility-wide security measures. Select *Yes* or *No* as to whether or not there are security measures related to the RBPS for this asset. If the facility answers *Yes* to having asset-specific security measures for a particular RBPS, then the facility must answer the questions related to that RBPS.

A facility must address RBPS 2 for each asset whether or not the facility previously entered facility-wide security measures. This is where a facility should identify security measures specific to each asset.

When identifying security measures, select the security measures that most accurately and completely describe the ***existing*** asset level security measures. Where the facility believes the security measures provided by the SSP tool do not accurately or completely depict its security measures, the facility should select *Yes* for *Other* and describe/explain this security feature in the *Other* text box provided.

5.1.3 Planned and Proposed Security Measures

At the end of each RBPS section, the facility is able to provide information on any Planned and Proposed security measures for the facility and any other assets the facility may identify. DHS may consider a planned security measure in determining whether an SSP satisfies an applicable RBPS if the measure:

- Is in the process of being installed; or
- Is in the design phase but has an approved and documented capital budget; or
- Is in the bid process and has been placed for bid or bids have been received and are under review; or
- Is in a pilot phase or is in execution as a demonstration project, and for which there is a general but documented implementation budget and schedule.

If a facility provides information about a planned security measure for consideration by DHS, the facility should also expect to produce documentation that supports the planned measure, such as evidence there is funding. DHS will consider planned measures during the SSP approval process. A proposed measure is one that is under consideration by the facility for implementation but is not yet a planned measure, and will not be considered by DHS in determining whether to approve an SSP.

Proposed Measures

A facility can provide three types of information using this section of the SSP tool: Proposed Security Measures the facility wants to share with DHS; Existing Security Measures the facility is proposing to eliminate or remove; and Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

Entering Proposed Security Measures

If a facility chooses to share its proposed security measures with DHS, then the facility should enter a

description of the proposed security measure for this asset. The facility should label each proposed security measure using "Proposed Security Measure X" where the X would be a number for the Proposed Security Measure. A sample entry for a Proposed Security Measures could be: "Proposed Security Measure 1 – Install new 8 feet high brick wall with 1 foot of barbed wire topping at Asset 1; Proposed Security Measure 2 – Install an anti-vehicle wedge with a Department of State Rating of 4 at Asset 1's main entry gate." The facility can provide as much detail as necessary to convey each Proposed Security Measure to DHS.

Entering Proposals to Eliminate Security Measures

Facilities may list and/or describe existing asset-specific security measures as part of Section 5 of their CSAT SSP submissions. Existing security measures which each covered facility describes or lists in its CSAT SSP submission may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. However, this section of the CSAT SSP tool will provide facilities the opportunity to disclose that certain existing security measures are proposed to be removed or eliminated in the future. Of course, if a facility chooses to eliminate an existing security measure that is relevant to one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

If a facility chooses to share its proposals to eliminate security measures with DHS, then the facility should enter a description of the proposed security measure that will be eliminated from this asset and include a timeframe for when that security measure will be eliminated. The facility should label each proposed security measure to be eliminated using "Proposed Elimination X" where the X would be a number for the proposed security measure to be eliminated. A sample entry could be: "Proposed Elimination Measure 1 – Remove existing 4 feet high chain link fence around Asset 1 by September 2012; Proposed Elimination Measure 2 – Remove magnetic locks to the main gate for Asset 1 by December 2015." The facility can provide as much detail to DHS as necessary to convey each proposed security measure to be eliminated.

Entering Proposals for Specific Security Measures Not to be Included in SSP

Facilities may list and/or describe existing asset-specific security measures as part of Section 5 of their CSAT SSP submissions. Existing and planned security measures which each covered facility describes or lists in the asset-specific portions of its CSAT SSP submission may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. However, this section of the CSAT SSP tool will provide facilities the opportunity to propose that certain existing and/or planned security measures identified in this tool not be considered by DHS in evaluating their Saps for approval. Of course, if a facility chooses not to include an existing or planned measure that is relevant to satisfaction of one or more CFATS RBPS in its SSP, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

If a facility would like to identify existing or planned security measures in the CSAT SSP tool for a specific RBPS, but does not want DHS to consider those measures during its evaluation of the facility's SSP, the facility should make a note of the question numbers that correspond to those particular security measures. The facility should use this text box to enter a description of the security measures the facility does not want to be considered by DHS. The facility should label each specific security measure not to be included by using "Security Measure Not to be Included in SSP X [Q:#.#-#####]" where the X would be a number for the specific security measure not to be included and [Q:#.#-#####] is the question number found in the SSP tool that is related to the specific security measure not to be included. A sample entry could be, "Security Measure Not to be Included in SSP 1 – [Q:28.04-16034] Facility does not want its fence barrier around Asset 1 considered by DHS during evaluation of its SSP; Security Measure Not to be

Included in SSP 2 – [Q:28.05-16037] Facility does not want its 1 feet high barbed wire top guard at Asset 1 considered by DHS during evaluation of its SSP.

Completing the Asset-Specific Security Measures Section. When the facility is finished entering the security measures for an asset, the user will return to the Asset Screen where he/she will be able to provide information on additional Assets, if needed.

5.2 Completing RBPS for All Assets

When the facility has entered all of the asset-specific security measures by RBPS for an asset, the user is directed back to the original Asset Screen. A facility may name and describe additional assets at this point. If the facility has entered the specific security measures for all of its assets, answer *Yes* to the question **Have all assets been listed and details provided?**

6.0 SSP Completion

Preparer: After entering all of the relevant data, the user will see the SSP Completion screen. At this point, the Preparer is advised to both validate the information and review it for completeness and accuracy.

Validate Report. A validation check for basic logical errors is done by clicking on *Validate Report* on the menu on the left. Information that is missing or incorrectly formatted will be listed and highlighted in red and a link will be provided to take the user to the affected area to fix the error or add the missing information. Once the information has been corrected, click *Validate Report* again to check for any additional errors.

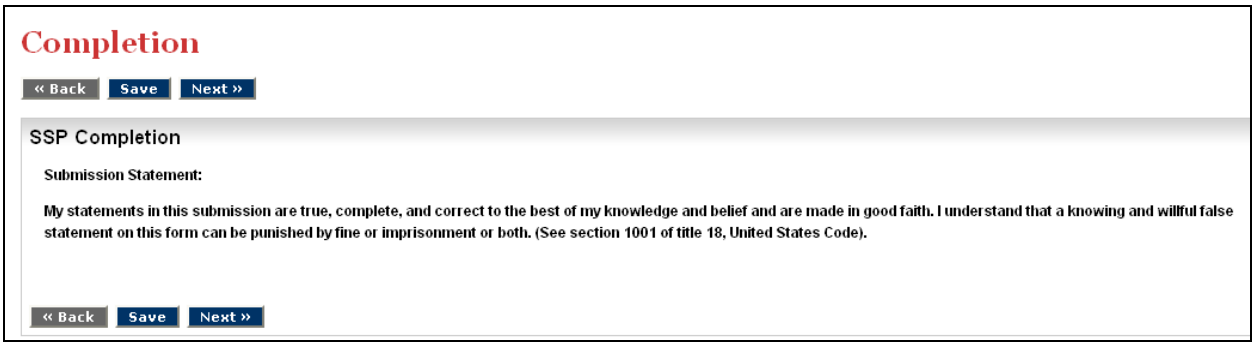

Figure 6-1 – SSP Completion

The SSP tool will not find and highlight errors other than missing required data or logical errors (e.g., unrecognized characters such as commas or percent signs). Users are advised to print a Summary Report and review all of the information for accuracy even if no validation errors appear on the Validation Report.

View Summary Report. Click on *View Summary Report* on the menu on the left and the SSP tool will generate a report showing the questions and the data entered. This report is a PDF and can be printed or saved.

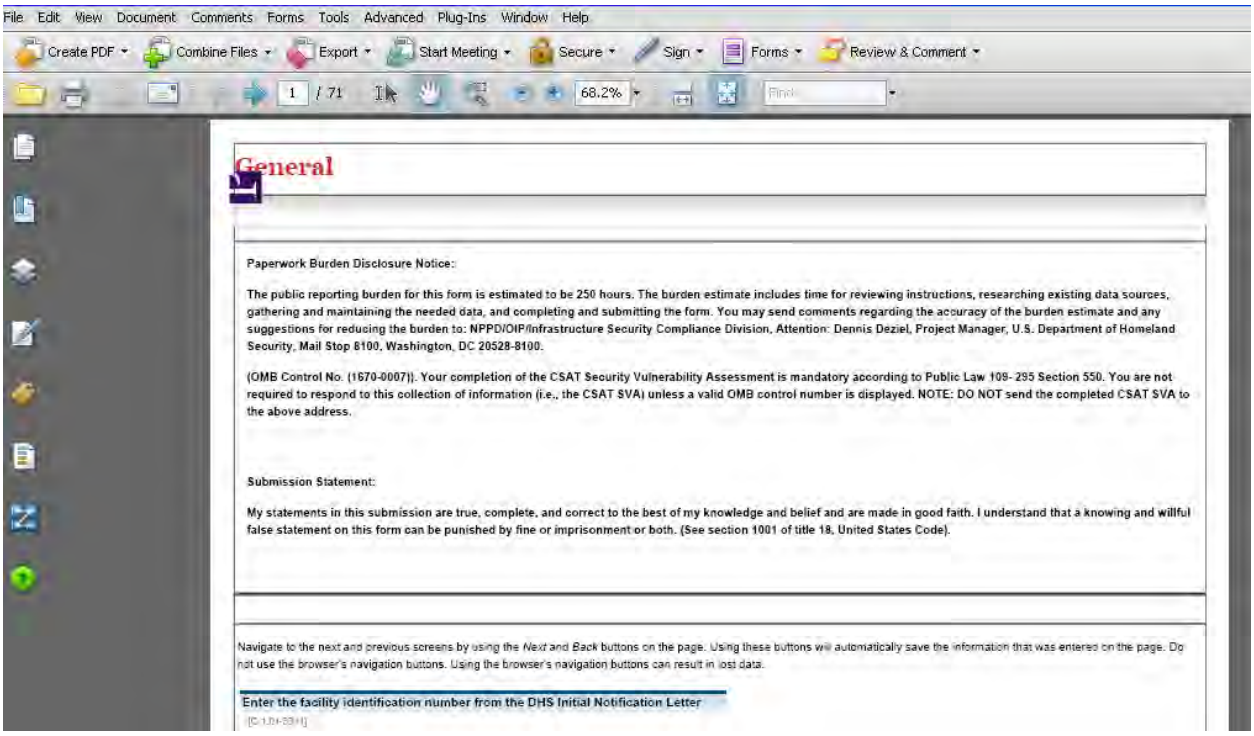

Figure 6-2 Summary Report

When the report has been successfully validated and reviewed, click *Next* to continue the completion process.

Note: If the Preparer is also the Submitter and has only one username, the screen presentation will be similar to the Submitter screens detailed below. The Preparer will not have the option to transfer the account to the Submitter; instead, the CSAT system will direct the Preparer to submit the completed SSP directly to DHS.

Transferring Answers to Submitter. Click the *Transfer to Submitter for Review* button to transmit the SSP to the Submitter for review. The Preparer can also choose to have a copy of the letter acknowledging receipt of the SSP sent to the submitter as well. [Q:1.92-13719] A *Yes* answer will send an email notifying the Preparer that the survey has been transmitted to the Submitter for review. Once the SSP is sent to the Submitter, the Preparer has read-only access to the data unless the Submitter sends the SSP back for revision (at which point the Preparer may again edit and enter data).

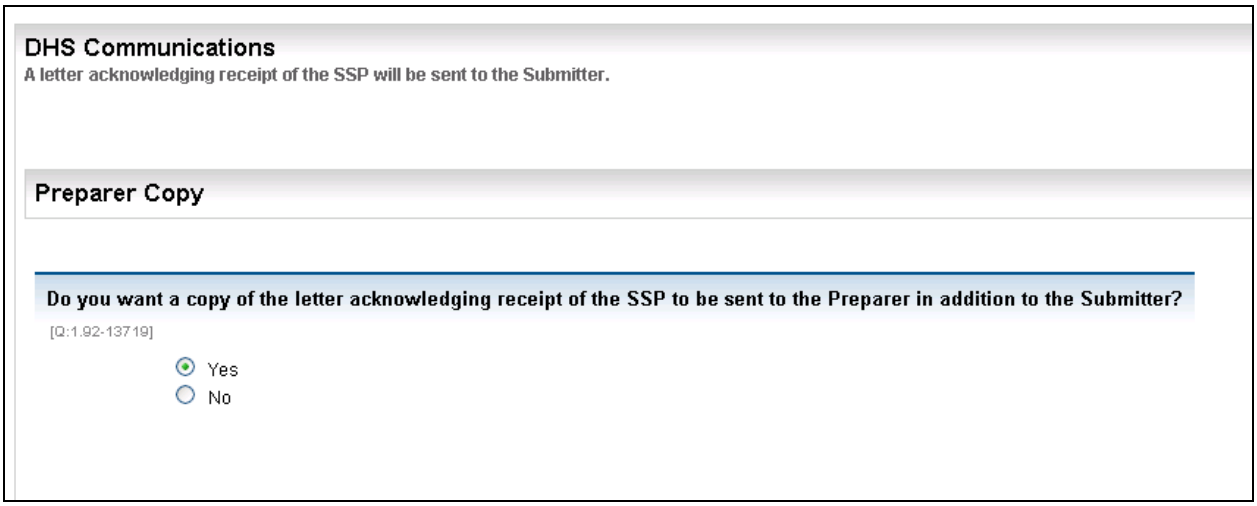

Figure 6-3 – DHS Communications

Submitter Review: Once the Preparer has submitted the completed SSP, the Submitter will receive an email notifying him/her that the SSP is ready for review. When the Submitter enters the CSAT system, the system will display the facility or facilities that the Submitter is authorized to review. The Submitter will see, on the CSAT landing page (Figure 1-1), the facility's status in the process (*In Review* will be listed for completed surveys awaiting final review and submission). Click the name of the facility to review.

The Submitter may now page through the SSP and view and edit the answers supplied by the Preparer. After reviewing all of the information, the Completion Screen will be displayed. The Submitter can now return the survey to the Preparer for modifications (click the *Transfer to Preparer for Modifications* button) or proceed to the *Final Validation*.

If the SSP is returned to the Preparer, its status will return to *In Progress* on the initial sign-in screen and the Preparer and Submitter will receive emails to that effect with instructions on next steps for continuing the SSP completion and submission process.

To finish the SSP, click *Final Validation* and correct any errors or omissions. When the validation is complete, click *Continue*.

The Submitter must retain a copy of the completed SSP for the facility's record as specified in 6 CFR §27.255(b). Once the facility submits the SSP to DHS, a facility no longer has access to it. A submitted copy of the SSP will be helpful in case the data needs to be re-entered. This printed or electronic record is CVI and must be protected as CVI. Users can create a copy of the completed SSP by clicking on the button *Print Version of SSP*. The user can then choose to print the PDF (*File>Print*) and to save it electronically (*File>Save*). After saving and printing a copy for your files (and checking that the copy is legible), the Submitter should click *Submit to DHS* to officially submit the completed SSP. **[NOTE: Be sure to read carefully and understand the Submission Statement on this page of the SSP tool before submitting the SSP.]**

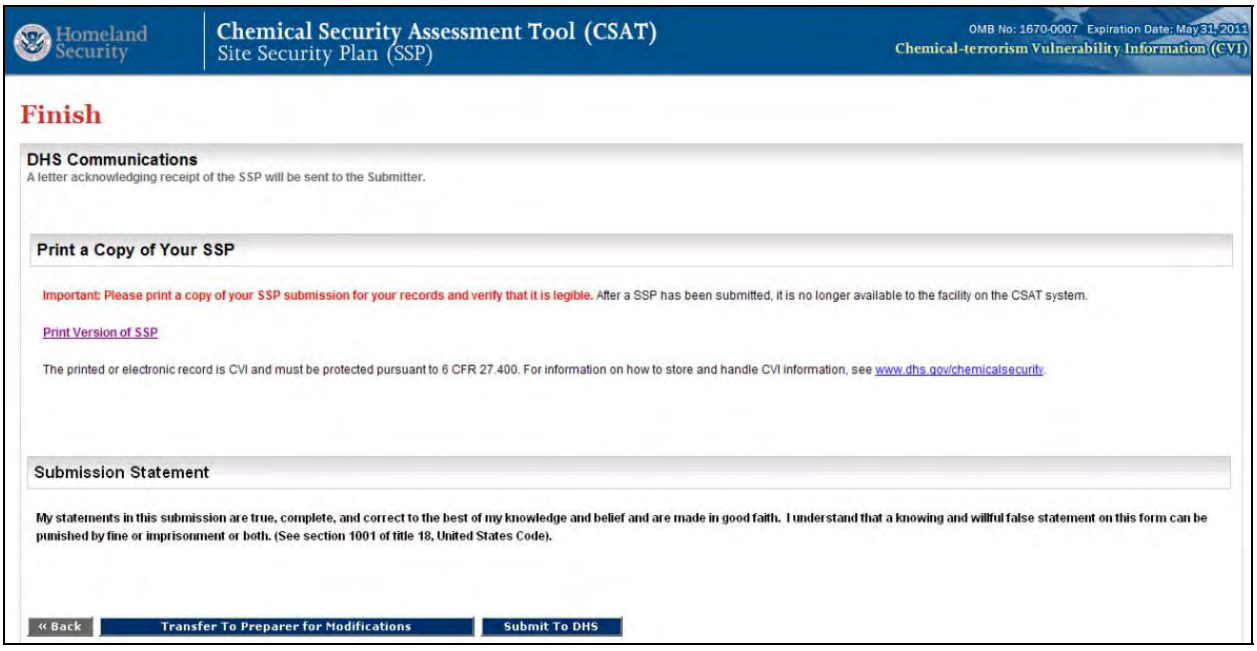

Figure 6-4 – Finish

SSP Tool Complete

List of Acronyms Used in the Site Security Plan Instructions

ASP	Alternate Security Program
CCPS	Center for Chemical Process Safety
CCTV	Closed-Circuit Television
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
COI	Chemical(s) of Interest
CSAT	Chemical Security Assessment Tool
CVI	Chemical-terrorism Vulnerability Information
CW/CWP	Chemical Weapons/Chemical Weapons Precursor
DCS	Distributed Control Systems
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
EPA	Environmental Protection Agency
EXP/IEDP	Explosive/Improvised Explosive Device Precursor
FAQ	Frequently Asked Question
ICS	Industrial Control Systems
IED	Improvised Explosive Device
IEDP	Improvised Explosive Device Precursor
IFR	Interim Final Rule
IMS	Intrusion Monitoring System
IT	Information Technology
NAICS	North American Industrial Classification System
PCS	Process Control Systems
RBPS	Risk-Based Performance Standards
RMP	Risk Management Plan
SCADA	Supervisory Control And Data Acquisition
SSP	Site Security Plan
STQ	Screening Threshold Quantity
SVA	Security Vulnerability Assessment
UPS	Uninterruptible Power Supply
VBIED	Vehicle-Borne Improvised Explosive Device
WME	Weapon of Mass Effect