

CSAT Security Vulnerability Assessment Application

Instructions

January 3, 2011
Version 2.1



Homeland
Security

Table of Contents

1.	Overview	1
1.1	Chemical Facility Anti-Terrorism Standards	1
1.2	The Security Vulnerability Assessment Process	2
1.3	Getting Additional Help	2
2.	Getting Started	3
2.1	Chemical-Terrorism Vulnerability Information	3
2.2	CSAT User Roles	3
2.3	SVA Information and Resources	4
3.	Using CSAT	6
3.1	Accessing CSAT	6
3.2	Adding/Deleting Reviewers	7
3.3	Updating Facility Information	8
3.4	SVA Survey Navigation	9
3.4.1	Navigation Buttons.....	9
3.4.2	Navigation Menu.....	11
3.5	Entering SVA Data.....	11
3.5.1	Saving Data	12
3.5.2	Validating Data	13
3.6	SVA Pre-Population from Top-Screen.....	13
4.	General Facility Information	15
4.1	Facility Information Details	16
4.2	Updating Facility Information	17
4.3	Facility Map.....	20
4.3.1	Uploading Images.....	22
4.4	Tier 4 Status and Alternate Security Program Submission	23
4.4.1	Uploading Alternate Security Program Documents	25
4.4.2	Uploading Plot Plans/Maps	27
4.4.3	Completing Alternate Security Program Submission	29
5.	Facility Security Issues	30
5.1	Reporting Facility Security Issues	30
5.2	Reporting Chemicals of Interest	32
5.3	Summary of Facility Security Issues.....	34
5.4	Facility Characteristics.....	35
5.5	Facility Security Information	35
5.5.1	Facility Security Equipment	36

CSAT Security Vulnerability Assessment Application Instructions

5.5.2	Additional Security Equipment.....	38
5.5.3	Utility Systems and Infrastructure Support	40
5.5.4	Additional Utility Systems	41
5.5.5	Inventory Control Measures	42
5.5.6	Personnel Access Control Measures	44
5.5.7	Additional Personnel Access Controls.....	47
5.5.8	Shipping and Receiving Control Measures	48
5.5.9	Post-Release Measures and Equipment.....	50
5.5.10	Additional Post-Release Measures	52
5.5.11	Site Vulnerability Factors.....	53
6.	Asset Characterization.....	56
6.1	Identifying Assets.....	56
6.2	Characterizing Assets.....	59
6.2.1	Chemical of Interest Associated with an Asset	61
6.2.2	Detailed Asset Chemical of Interest Information	62
6.2.3	Cyber Control and Business Systems.....	72
6.2.4	Asset Completion.....	73
6.3	Cyber Control Systems.....	74
6.4	Cyber Business Systems.....	75
7.	Vulnerability Analysis	77
7.1	Facility Security Issues Analysis.....	77
7.2	Introduction Screen.....	78
7.3	Asset Location	79
7.4	Attack Modes	81
7.4.1	Attack Scenario Selection.....	83
7.4.2	Attack Location Map	86
7.4.3	Attack Scenario Questions	87
7.4.4	Vulnerability Factor Questions.....	89
7.4.5	Release Questions	98
7.4.6	Completion of Vulnerability Analysis	100
8.	Computer Systems Analysis.....	101
8.1	Cyber Control Systems.....	101
8.1.1	Mapping Cyber Control Systems.....	101
8.1.2	Cyber Control System Questions	103
8.2	Business Control Systems.....	105
8.2.1	Mapping Business Control System.....	106
8.2.2	Locating Offsite Business Systems	107

CSAT Security Vulnerability Assessment Application Instructions

8.2.3	Business System Questions	107
9.	SVA Completion.....	110
9.1	Validating Reports	110
9.2	Summary Reports.....	111
9.3	Transferring to Submitter	111
9.4	Submitter Review.....	112
	Appendix A: Acronyms Reference List.....	114

1. Overview

This document provides instructions to facilities for completing and submitting the Security Vulnerability Assessment (SVA) through usage of the Chemical Security Assessment (CSAT). The instructions detail how to complete an SVA in accordance with requirements of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27. This document also provides instructions on how to submit an Alternative Security Program (ASP) for those that are authorized to do so. **NOTE:** These instructions apply **only** to the CSAT SVA application.

All examples provided in this document are illustrative and are merely intended to highlight specific points within the CSAT SVA application. Each facility must carefully consider its own unique characteristics and circumstances to determine the relevance and appropriateness of each example.

1.1 Chemical Facility Anti-Terrorism Standards

Section 550 of the DHS Appropriations Act of 2007, Pub. L. 109-295 (hereby referred to as “Sec. 550” or “the Act”), authorizes the Department of Homeland Security (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. 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. As provided by 6 CFR § 27.215, the CSAT SVA application is one method DHS uses to gather such information from high-risk facilities.

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 of 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 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 application to complete its SVA. (See 6 CFR § 27.215 for more details.) Each Tier 4 facility may use the CSAT SVA application 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 the 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 not subject to CFATS (barring a change to the facility's circumstances which would change it to high-risk). For each facility that is confirmed to be high-risk, DHS will provide a Final Notification Letter which specifies the facility's final tier. The facility then must complete

and submit a Site Security Plan (SSP) under 6 CFR § 27.225 or an Alternative Security Program (ASP) in lieu of a SSP, as provided by 6 CFR § 27.235.

1.2 The Security Vulnerability Assessment Process

The CSAT SVA application allows users to submit information through the following process:

1. The application collects basic facility identification information.
2. The application collects information about the chemicals that a facility possesses.
3. The application collects information about assets at the facility that involve the COIs identified by DHS in the DHS initial notification letter.
4. The application enables users to locate assets on an interactive map and requires that the user apply DHS attack scenarios, or define attack scenarios of his/her own, to run against his/her facility's assets. The application uses the attack scenarios to provide DHS with data on the vulnerability and consequentiality of such attacks. The user will assess the vulnerability of his/her facility based on the security measures already in place at the facility.
5. Finally, the application collects information on relevant cyber systems that may affect the security of identified assets.

NOTE: If a SVA submitted by a facility is rejected by DHS for any reason or the facility needs to repeat the SVA process, all of the information must be re-entered into CSAT. Therefore, the facility should retain a copy of its completed SVA. See Section 9 for directions on how to print out a copy of the SVA before it is submitted to DHS.

1.3 Getting Additional Help

- The CSAT Help Desk has a toll-free number that users can call with questions regarding the CSAT SVA application. 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.
- More details on 6 CFR Part 27, information regarding Chemical-Terrorism Vulnerability Information (CVI), and other related information is available on the DHS Web site at <http://www.dhs.gov/chemicalsecurity>.

2. Getting Started

A facility must first register with DHS to access the CSAT application. Facilities that have submitted CSAT Top-Screens have already registered and been assigned the user roles which are listed below in Section 2.2. Individuals who retain the user access roles that were previously assigned to them for completion of the Top-Screen will need them to prepare and submit the CSAT SVA.

2.1 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. (Please see 6 CFR § 27.400 for more details.)

All information entered into the CSAT SVA application is CVI. Likewise, both the information maintained by DHS (on servers prior, during, and after submission of the SVA) and the resulting SVA determination that DHS prepares and shares with a facility are CVI and will be marked accordingly. Every CSAT user **must** complete CVI training to become a CVI Authorized User prior to entering information into the CSAT SVA Application. CVI training addresses how to protect information submitted through the CSAT SVA application as well as to whom and under what circumstances such information may be disclosed. The DHS CVI training is available from a link on the CVI training page on the DHS Web site, http://www.dhs.gov/xprevprot/programs/gc_1185556876884.shtm. A user will **not** have access to the CSAT SVA application until the user has completed CVI training and is a CVI authorized user.

Only information developed, submitted, or maintained pursuant to CFATS and Section 550 is considered CVI; thus, information previously developed under other statutory regimes or for a facility's own business purposes may not be considered CVI (see CFATS IFR preamble, 72 FR 17715). Therefore, some of the existing information used by a facility to complete the SVA may not be CVI. For more details regarding what information is and is not CVI and the procedures for protecting CVI, please refer to the DHS CVI Procedures Manual, which is available at <http://www.dhs.gov/chemicalsecurity>.

2.2 CSAT User Roles

A variety of individuals for each facility 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 by the facility through the CSAT system.

CSAT User Role	Description
Preparer	A user who is authorized to enter the data into the CSAT system and can designate the SVA as ready for review by the Submitter. When the Preparer sends the SVA to the Submitter for review, the Preparer will no longer be able to edit the information in the SVA unless the SVA is returned to the Preparer by the Submitter for revision.
Submitter	A user who is designated by the facility to submit the information collected in the CSAT system to DHS. When the Submitter has access to the SVA, he/she may revise the information contained therein.
Authorizer	A user who provides assurance to DHS that the Submitter and Preparer are authorized to complete the CSAT information. The Authorizer is allowed to review information in the SVA but not to enter, edit, or submit the information, unless he or she is also the Preparer or Submitter.
Reviewer	A user who is allowed to review information but not to enter, edit, or submit the information. A Reviewer does not have edit or approval privileges and must be invited by a known user from within the Top-Screen. Upon logging in, the Reviewer must agree to all use requirements and to the CVI Non-disclosure Agreement/Authorizing Statement.

Table 2.1: CSAT User Role Descriptions

- It is the responsibility of each facility to organize and manage the individuals and teams of individuals who contribute to its CFATS compliance, particularly during the completion and submission of the SVA.
- Once the Submitter transmits the SVA to DHS, it is no longer accessible to the facility or its designated Preparer, Authorizer, Reviewer, or Submitter.
- For additional information about CSAT user roles, including instructions on assigning, transferring and consolidating roles, please see the CSAT User Registration Guide and Account Management Guides, which are available at http://www.dhs.gov/xprevprot/programs/gc_1169501486197.shtm. The CSAT Help Desk can also provide further information on users and user roles for purposes of completing the SVA.

2.3 SVA Information and Resources

Prior to accessing CSAT and entering information into the SVA application, DHS recommends that a facility collect and verify for accuracy and completeness the following information:

- A copy of 6 CFR Part 27, which is available at <http://www.dhs.gov/chemicalsecurity>.
- A copy of the 2007 DHS COI list with STQs (Appendix A to 6 CFR Part 27), which is available at <http://www.dhs.gov/chemicalsecurity>.

CSAT Security Vulnerability Assessment Application Instructions

- A copy of the CVI Procedural Manual regarding protection of CVI, which is available at <http://www.dhs.gov/chemicalsecurity>.
- A copy of the DHS initial notification letter that was sent to the facility regarding its initial status as a high-risk chemical facility, its preliminary tier assignment, and a listing of its COI that must be addressed in the SVA.
- A copy of the facility's submitted Top-Screen, which is a CVI document.
- A copy of the DHS CFATS Attack Scenario Descriptions, which is a CVI document and is available at csat.dhs.gov/csats.
- Chemical inventory information, including the names and quantities of all DHS COI which are manufactured, processed, used, stored, or distributed at the facility, and the location of assets related to the COI identified in the DHS initial notification letter.
- A copy of any recent SVA or SSP which may have been completed by the facility.

3. Using CSAT

3.1 Accessing CSAT

The initial notification letter that DHS sends to your facility will have instructions for accessing the CSAT SVA application. When you go to the CSAT site, it will prompt you to enter your user name and password. Once you have accessed CSAT, the following screen will appear:

Choose a survey to edit or review.

Chemical Facility
 123 Main Street
 Argonne, IL 60439
 Facility ID: 24107

[Update Facility Info](#)
[Manage User Roles](#)

Survey Type	Status	Start Date	End Date	Survey ID	Summary Report
SVA	New			34898	Edit/Review

Picture 3.1: CSAT Survey List Screen

The **CSAT Survey List** screen lists each registered facility to which you are assigned and the associated surveys to which you have access, including Top-Screens. This screen presents you with three options:

- 1) Accessing the SVA survey for a given facility;
- 2) Managing user roles for any of the facilities displayed; and/or
- 3) Updating facility information with a new name or address.

NOTE: Your CSAT session will time out after 20 minutes if the system is not in use. If that happens, you will need to log back in to CSAT to restart you session. Data you have saved will not be lost, and your new session will open on the same screen where your previous session ended.

3.2 Adding/Deleting Reviewers

Submitters, Preparers, and Authorizers can add or delete Reviewers to an SVA. To add new users, click the [Manage User Roles] button on the left side of the **CSAT Survey List** screen. The following screen will appear:

[« Return to CSAT Survey List](#)

Facility 1

This page manages user access to the CSAT surveys for **Facility 1**.
To transfer your roles to another person, please use the [Manage My Account](#) application.

Active Survey	Authorizer (All Surveys)	Submitter (All Surveys)	Preparer(s)	Reviewer(s)
Top-Screen Not active				No reviewers.
SVA Survey ID: 38021	Laura Demo (laura.demo)	Laura Demo (laura.demo)	Q	No reviewers. Add Reviewer
Site Security Plan Not active				No reviewers.

Picture 3.2: CSAT User Management Screen

A Reviewer with read-only privileges may be added to each facility. Reviewers added during the Top-Screen will have their privileges to view a Top-Screen for a specific facility carried over into the SVA and SSP for that same facility, but Reviewers added to the SVA survey will not be able to view any new Top-Screens that may be generated in the future. **NOTE:** Authorizers, Submitters and Preparers **should not** grant themselves Reviewer privileges. Doing so will disable **all** editing privileges.

- To add a Reviewer, click the [Add Reviewer] button to the right of the survey for which you would like to add the Reviewer. A new screen will appear:

CSAT Security Vulnerability Assessment Application Instructions

This process will grant read-only access to this survey to the individual specified as a Reviewer by one of the following methods:

Existing User Choose this option if the person to whom you wish to grant Reviewer access to already has a CSAT account. This method will automatically give the specified Reviewer access to this survey. Grant Access to Existing CSAT User
New User Choose this option if the person to whom you wish to grant Reviewer access to does not have a CSAT account. This method will generate a CSAT user account for this person and email the username and password to him/her. Grant Access to New CSAT User

Picture 3.3: CSAT Reviewer Access Screen

The **CSAT Reviewer Access** screen will ask 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 the appropriate button—[Grant Access to Existing CSAT User] or [Grant Access to New CSAT User]—and entering the requested information.

- To delete a reviewer, click the [Delete] button.
- When you are finished, click the [Return to CSAT Survey List] button to return to the **CSAT Survey List** screen.

3.3 Updating Facility Information

To update information for a facility, including its name and/or address, click the [Update Facility Info] button **CSAT Survey List** screen. The following screen will appear:

Register a
New Facility
Link

Update Facility Information

Use the form below to make changes to this facility's name, location, or other information. Do not change this facility's information to that of a different facility. If you need to add a new facility, [register a new facility](#).

Facility Address

Facility Name

Tim's Chemical Facility

▲ Provide the name of the facility. The name must be specific to the facility; if the facility is part of a large corporation, the name may be the corporate name plus the location (for example, "ABC OilRefining - Hightown Plant").

Alternate Facility Name

▲ Provide alternative names under which the facility may be known.

Add

Street Address

123 Main Street

▲ Enter the street address of the facility's physical location. [Note: This may be different from the mailing address.] Use local street and road designations, not post office or rural box numbers.

Street Address (continued)

Street Address (continued)

City

Argonne

▲ Enter the city of the facility's physical location. [Note: This may be different from the mailing address.]

State

Illinois

▲ Select the state of the facility's physical location. [Note: This may be different from the mailing address.]

ZIP Code

60439

▲ Enter the ZIP Code (including the 4 digit extension, if applicable) of the facility's physical location. For example, XXXXX or XXXXX-XXXX are valid ZIP Code formats. [Note: This may be different from the mailing address.]

County

▲ Provide additional county names in which this facility is located.

Add

Parent Company

The parent company is the corporation or other business entity that owns greater than 50 percent of the voting stock of the company. If the facility is owned by a joint venture, enter the first of the two major owners here. If the company does not have a parent company, leave these fields blank.

Parent Company 1 Name

Parent Company 1 DUNS

Parent Company 2 Name

Parent Company 2 DUNS

Co-location

Picture 3.4: Update Facility Information Screen

The information displayed on the **Update Facility Information** screen is populated from previous updates. You can also access the **Update Facility Information** screen while using the CSAT SVA application. Please see Section 4.2 for more details.

- When you are finished updating your facility's information, click the [OK] button on the bottom of the screen to save your updates.
- To leave the screen **without** saving your updates, click the [Cancel] button on the bottom of the screen.
- **NOTE:** Do **not** use this screen to enter a new facility. If a new facility needs to be registered, click the [register a new facility](#) link at the top of the screen.
- **NOTE:** A facility's coordinates (latitude and longitude) cannot be changed from within CSAT. Please contact the CSAT Help Desk to process coordinate changes.

3.4 SVA Survey Navigation

3.4.1 Navigation Buttons

You can navigate within the CSAT SVA survey by using the [Next] and [Back] buttons on the screen.



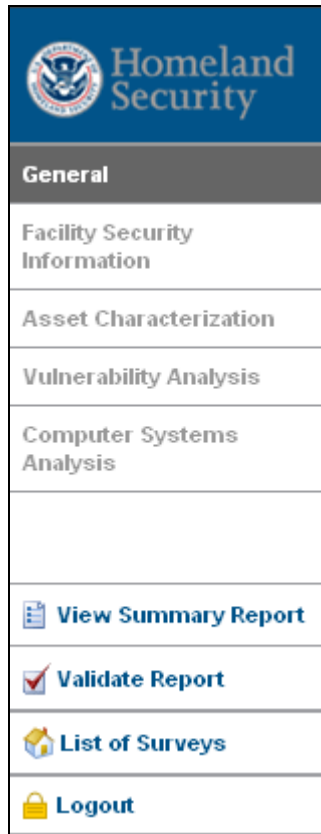
Picture 3.5: SVA Survey Navigation Buttons

- Using the [Next] and [Back] buttons will automatically save the information that you entered on any given page within the survey.
- If you have entered information on a CSAT screen but do not intend to go to another screen, click the [Save] button to retain the information.
- **NOTE:** Do *not* use the [Back] button (or arrows) in your Web browser to navigate through CSAT. Using your browser's navigation buttons can result in lost data.

Please note that if you return to a section of the SVA that was previously completed, you will need to use the [Next] button to review all of the subsequent pages. The CSAT system adapts the SVA screens presented for completion based on the answers provided on previous pages; thus, a change to one section of a SVA might require you to answer additional/different questions in another section.

3.4.2 Navigation Menu

While completing the SVA, a navigation menu will appear on the left side:



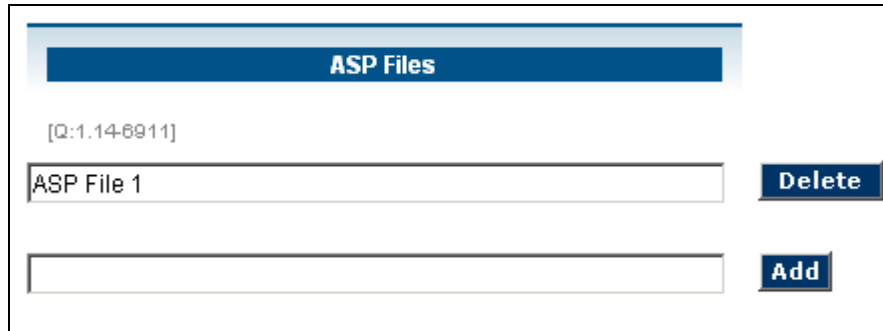
Picture 3.6: SVA Survey Navigation Menu

You can navigate through the SVA by selecting the desired topic in the navigation menu.
NOTE: You can only select the menu commands that are displayed in **bold blue text**.

3.5 Entering SVA Data

- Each section of the SVA will be highlighted once it has been completed.

- On some screens, you will need to enter additional text into text boxes to complete the response to a question. When you are finished entering text, use the [Add] button next to the text box to save your information. If you decide to empty a text box of the text you have entered, use the [Delete] button next to the text box. See Picture 3.7 for an example.

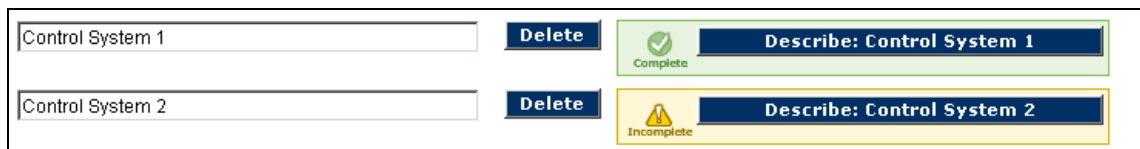


The screenshot shows a section titled "ASP Files" in a blue header. Below the header, there is a question identifier "[Q:1.14-6911]". There are two rows of input fields. The first row contains a text box with the text "ASP File 1" and a blue "Delete" button to its right. The second row contains an empty text box and a blue "Add" button to its right.

Picture 3.7: Text Boxes and Buttons

- On screens where further explanation of an item is required, a [Describe] button is provided. Click the button to answer additional questions specific to that item. At the conclusion of these additional questions, you will be asked to select a check box to verify that the description you provided is complete. When you indicate that the questions are complete, you will be returned to the original list of items.
 - If you marked the item as being complete and all required questions were answered for that item, the item will be displayed with a green **Complete** 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 **Incomplete** icon.



The screenshot shows two rows of items. Each row has a text box on the left, a blue "Delete" button in the middle, and a "Describe" button on the right. The "Describe" button for "Control System 1" is highlighted with a green border and a green checkmark icon, indicating it is complete. The "Describe" button for "Control System 2" is highlighted with a yellow border and a yellow warning icon, indicating it is incomplete.

Picture 3.8: Description Buttons and Icons

3.5.1 Saving Data

All of the information you enter into the SVA survey is saved when you click the [Save] button, or when you click either the [Next] or [Back] button. You can exit and return to CSAT multiple times until your SVA is complete; the information that has been saved during the previous session will be available to you upon re-entry into the SVA. See Section 3.4.1 for more details.

3.5.2 Validating Data

Data validation ensures that you have entered your information in the correct format (e.g., that a phone number is numeric and formatted correctly). You can perform some basic data validation by reviewing the information you entered in a screen before moving to another screen. You can perform a more thorough data validation by selecting the **Validate Report** option on the CSAT SVA survey navigation menu, as seen in Picture 3.6. The **Validate Report** option is also done automatically before SVA submission.

Using the **Validate Report** option provides a more complete information review. A **Validate Report** error message will be displayed if required data input fields are empty or incomplete, and you will be allowed to return to the error and correct it. For example, an error message will be displayed if the ID number of the facility is not entered (see Picture 3.9). The link provided on the error message will direct you to the input area for correction.

General

Missing or Invalid Entry!

- Missing answer to question, "Enter the facility identification number from the DHS Initial Notification Letter".

[Go to the page to address the issue listed above.](#)

Navigate to the next and previous screens by using the *Next* and *Back* buttons on the page. Using these buttons will automatically save the information that was entered on the page. Do not use the browser's navigation buttons. Using the browser's navigation buttons can result in lost data.

Enter the facility identification number from the DHS Initial Notification Letter

[Q:1.01-3311]

Does the DHS Initial Notification letter indicate that the facility is a Tier 4 facility?

[Q:1.01-3314]

☒ Yes

☐ No

Picture 3.9: Validate Report Error Message

NOTE: Data validation is performed **only** for logic and basic errors. Therefore, you should not expect the **Validate Report** option to ensure that your SVA has been completed without errors. Your Submitter is responsible for submitting accurate and correct information to the best of his/her knowledge.

3.6 SVA Pre-Population from Top-Screen

To ensure consistency, some questions in the SVA may be pre-populated with answers from the CSAT Top-Screen. Some answers will not be editable or, in some cases, viewable.

The following table provides a list of SVA questions that might be pre-populated with Top-Screen answers. If the questions listed below are not visible or editable in the CSAT SVA, the answers provided in the CSAT Top-Screen are being used. In some cases, answer pre-population cannot be completed and you will be required to answer the question. If the answers provided are no longer correct, please contact the CSAT Help Desk.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question
[Q1.01-3311]	Enter the facility identification number from the DHS initial notification letter.
[Q:1.0-3314]	Does the DHS SVA initial notification letter indicate that the facility is a Tier 4 facility?
[Q:2.0-971]	Does the DHS initial notification letter indicate that the facility should address security issues related to release-toxic COI?
[Q:2.0-3131]	Does the DHS initial notification letter indicate that the facility should address security issues related to release-flammable COI?
[Q:2.0-3132]	Does the DHS initial notification letter indicate that the facility should address security issues related to release-explosive COI?
[Q:2.0-3172]	Does the DHS initial notification letter indicate that the facility should address security issues related to theft/diversion of explosive/improvised explosive device precursor (IEDP) COI?
[Q:2.0-3171]	Does the DHS initial notification letter indicate that the facility should address security issues related to theft/diversion of weapon of mass effect (WME) COI?
[Q:2.0-3151]	Does the DHS initial notification letter indicate that the facility should address security issues related to theft/diversion of chemical weapon/chemical weapon precursor (CW/CWP) COI?
[Q:2.0-3173]	Does the DHS initial notification letter indicate that the facility should address security issues related to sabotage/contamination COI?
[Q:2.1-1037]	Select the release-toxic COI that are listed in the letter.
[Q:2.2-1038]	Select the release-flammable COI that are listed in the letter.
[Q:2.3-1039]	Select the release-explosive COI that are listed in the letter.
[Q:2.6-1043]	Select the theft/diversion EXP/IEDP COI that are listed in the letter.
[Q:2.5-1042]	Select the theft/diversion WME COI that are listed in the letter.
[Q:2.4-1041]	Select the theft/diversion CW/CWP COI that are listed in the letter.
[Q:2.7-1671]	Select the sabotage/contamination COI that are listed in the letter.
[Q:2.98-3411]	Have all of the security issues and chemicals of interest from the DHS initial notification letter been entered?
[Q:2.92-5911]	What is the surrounding topography of the facility?

4. General Facility Information

The first section of the SVA, the **General** section, requires you to provide facility information in data fields if they have not been pre-populated with CSAT Top-Screen information. The information requested in this section can be found in the DHS initial notification letter.

General

« Back Save Next »

Navigate to the next and previous screens by using the *Next* and *Back* buttons on the page. Using these buttons will automatically save the information that was entered on the page. Do not use the browser's navigation buttons. Using the browser's navigation buttons can result in lost data.

Enter the facility identification number from the DHS Initial Notification Letter

[Q-1.01-3311]

Does the DHS Initial Notification letter indicate that the facility is a Tier 4 facility?

[Q-1.01-3314]

☐ Yes
☐ No

Provide a short description of the functional operation of this facility, particularly with respect to the COI listed in your letter.

For example:
"this facility produces XYZ chemical as an intermediate product for further refining"
or
"this facility purchases XYZ chemical in bulk containers and packages it in retail containers for sale"

[Q-1.01-13011]

« Back Save Next »

Picture 4.1: SVA General Section Screen

4.1 Facility Information Details

The following table lists the questions that must be answered at the beginning of the **General** section, as well as details regarding how the questions should be answered.

Question #	SVA Question	Question Details
[Q:1.0-3311]	Facility Identification Number: Enter the facility identification number from the DHS initial notification letter.	DHS will assign each regulated facility a unique chemical security identification number. This number can be found in the DHS initial notification letter as well as on the CSAT launch page, shown previously in Picture 4.1.
[Q:1.0-3314]	Facility Tier Level: Does the DHS initial notification letter indicate that the facility is a Tier 4 facility?	• If so, answer Yes and follow the instructions on the next page to indicate if an ASP will be uploaded in lieu of completing the SVA. • Facilities with a preliminary tier level of Tier 1, Tier 2, or Tier 3 are not eligible to submit an ASP. In these cases, answer No and complete the CSAT SVA.
[Q: 1.01-13011]	Facility Description: Provide a short description of the functional operation of this facility, particularly with respect to the COI listed in your letter.	• Descriptions could be worded similarly to these examples: "This facility produces XYZ chemical as an intermediate product for further refining", or "This facility purchases XYZ chemical in bulk containers and packages it in retail containers for sale."

4.2 Updating Facility Information

The **General** section allows you to review and update your facility's information. Name, location and other facility information will be completed from previous surveys. Click on the [Update Facility Info] button to edit the address and provide other facility information. The table below provides more information on how to update facility information.

SVA Data Field/Question	Data Field/Question Details
Facility Information	• Facility Name: The name must be specific to your facility. If your facility is one of a corporation's multiple facilities, the name should be the corporate name and the location (e.g., "ABC Oil Refining — Hightown Plant"). • Alternative Facility Name: Provide any alternative name(s) by which your facility may be known (e.g., "Green Street Facility" or "Downtown Facility"). If your facility has no alternative name, leave this field blank. • Facility Location Address: Enter your facility's address for its physical location, including the street, city, state, ZIP code (with the four-digit extension, if applicable), and county. This address might not be the same as your facility's mailing address. Use local street and road designations, not post office or rural box numbers.
Parent Company	Enter the name and Dun and Bradstreet (DUNS) number of the corporation(s) or other business entity/entities (if any) that control 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, leave these fields blank and complete the Describe the facility's ownership text box provided.
Co-located Entities	Choose the appropriate description of the 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, or 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 company's facility, it is the sole tenant and you should select the <i>Not applicable</i> option button. • If a facility is host to a co-located tenant facility or is a co-located tenant facility, please provide the name and EPA RMP ID for each host/tenant facility. Add additional rows if necessary by clicking the [Add] button. • If the facility does not share its property with another facility, leave this field blank.

CSAT Security Vulnerability Assessment Application Instructions

SVA Data Field/Question	Data Field/Question Details
Security Vulnerability Assessment (SVA)	An SVA enables the identification and evaluation of security hazards, threats, countermeasures, and vulnerabilities. • If an SVA has been conducted for your facility, select the Yes option button and enter the methodology used for the SVA. • For facilities that have conducted an SVA previously, enter the date when the most recent SVA was completed at the facility. Use the following date format: mm/dd/yyyy (e.g., May 1, 2006 is entered as 05/01/2006).
Facility NAICS	Provide the five- or six-digit NAICS code that corresponds most closely to the primary activity of your facility as a whole. The first three digits of the code define a major business sector (e.g., 325 represents <i>Chemical Manufacturing</i>), and the last two or three digits indicate an establishment's specialty within the major sector (e.g., 325131 represents <i>Inorganic Dye and Pigment Manufacturing</i>). NAICS codes are maintained by the U.S. Census Bureau, and they can be found on its Web site at http://www.census.gov/epcd/naics02/.
Facility DUNS	Provide the facility's nine-digit DUNS number. This 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 the company's financial officer or corporate headquarters. It can also be located through the DUNS Web site at http://www.dnb.com.
EPA RMP Facility ID	If a 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 the acknowledgment letter to the facility. If a facility does not operate an RMP-covered process, leave this field blank.
Owner Name	Enter the name of the person or entity that owns the facility. 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; if the owner and operator are the same, enter the same information in both data fields.
Operator Name	Enter the name of the person or entity that is responsible for the daily operations of the facility. 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 owner; if the owner and operator are the same, enter the same information in both data fields.
Number of Full Time Employees	Enter the maximum number of employees. Provide the number of full-time (or resident) contractors at the facility at any given time, including shift changes. Do not include part-time or short-term workers, such as those who are brought in for turnarounds or construction, when determining this number. Do not use commas when entering data.

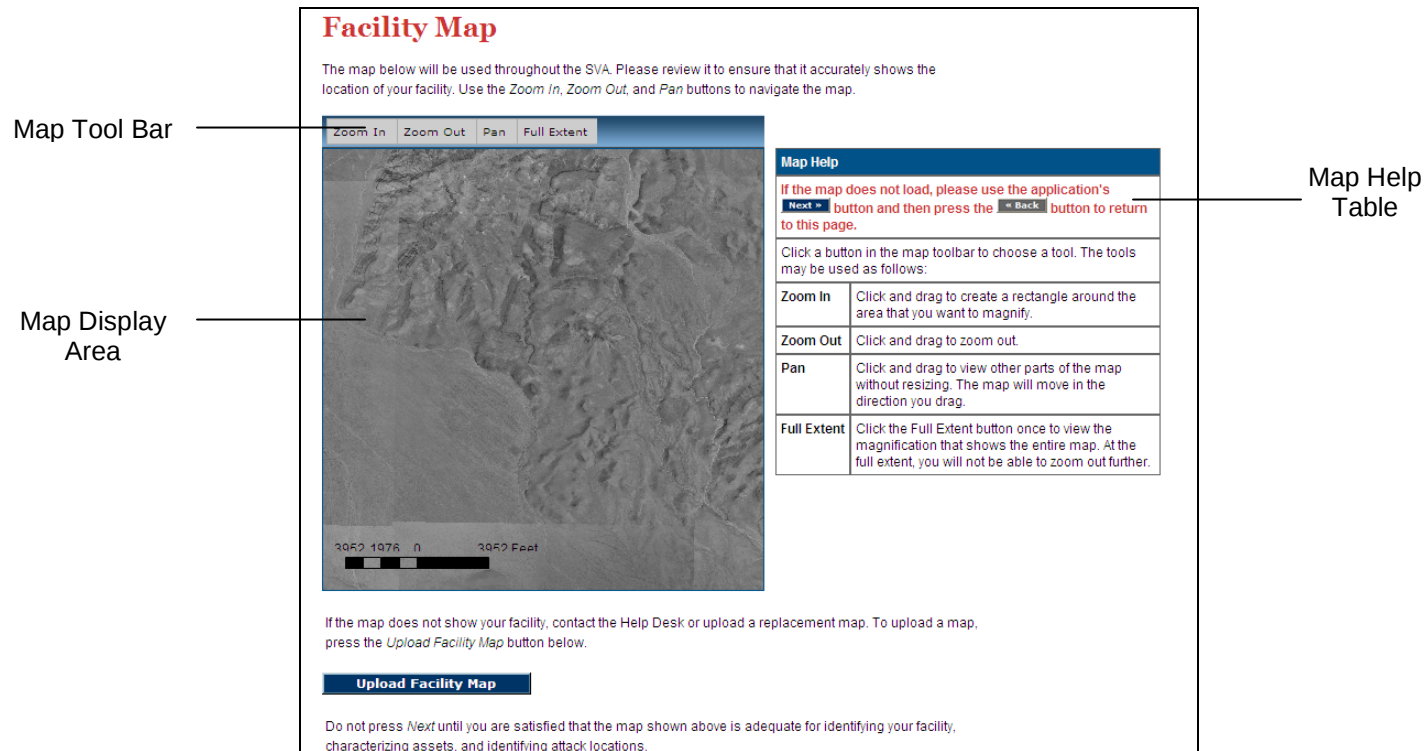
SVA Data Field/Question	Data Field/Question Details
Facility Coordinates	Please verify that the latitude/longitude coordinates are correct. Latitude and longitude cannot be changed on this screen; please contact the CSAT Help Desk to modify incorrect latitude and/or longitude information.

- When you are finished updating your facility's information, click the [OK] button on the bottom of the screen to save your updates.
- To leave the screen **without** saving your updates, click the [Cancel] button on the bottom of the screen.

NOTE: Special Handling of the Owner and Operator Names. During completion of the SVA, or at any point after submission of the initial Top-Screen, only one of these fields may be edited; once changed, the other field will become uneditable. For further clarification or help with updates, please call the Help Desk.

4.3 Facility Map

The **Facility Map** screen allows you to identify the location of the facility on an interactive aerial map of the subject facility and its immediate surrounding area. There are two primary features to assist the user with map navigation: the map tool bar and the associated map help table, which provides information on how to use the map tool bar.



Picture 4.2: Facility Map Screen

- The map tool bar features the following functions:
 - o **Panning:** Click the [Pan] button to navigate within the map to find the facility. After clicking [Pan], place your pointer within the map display area, hold down your left mouse button, and drag the map to the desired location. Click the [Pan] button again to deactivate the pan function.
 - o **Zooming In:** Click the [Zoom In] button to increase the magnification of the map display area where the facility is located. After clicking the [Zoom In] button, place your pointer near the place within the map display area you would like to magnify. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be magnified. You can continue to use this method to zoom to the level of magnification that is sufficient for locating the facility. Click the [Zoom In] button again to deactivate the magnification function.
 - o **Zooming Out:** Click the [Zoom Out] button if additional adjustment to the map display area is necessary to allow for a wider view. After clicking the [Zoom Out] button, place your pointer near the place within the map display area you would like to contract. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be contracted. Click the [Zoom Out] button again to deactivate the contraction function.
 - o **Full Extent:** Click the [Full Extent] button to reset the map to its fullest view. Repeat the steps described above until the facility is clearly identified.
- Once you are satisfied that the facility has been located and that you have successfully placed an image of the facility within the map display area, click the [Next] button at the bottom of the screen.

4.3.1 Uploading Images

If you cannot locate the facility on the map provided or the image of the facility you have found does not provide adequate detail, you have the option of uploading another image to better suit your needs. Click the [Upload Facility Map] button beneath the map display area, and a new screen will appear.

Upload Map Image

Use the form below to upload an image file that shows the **full extent** of your facility. The full extent image shall have enough detail to show buildings, roads, and docks, and is large enough to include all assets plus an area 950 feet beyond any asset. This image will be used as a map to allow you to specify the location of assets and attack scenarios. The pan, zoom in and zoom out features located on the map tool bar may be used to display the full extent of your facility.

Image of facility location:

Click the Browse... button to select an image file from your computer. Only one image file may be uploaded. The attachment must be less than 50MB in size, or it will not be accepted. The following file formats are accepted: BMP, JPEG, PNG, TIFF, GIF. The image must be a scale representation (not a logical diagram), show relevant buildings, roads, and docks, and include a large enough area to show all assets plus an area 950 feet beyond any asset.

Image dimensions units: Specify the units used for the Width and Height values below.

Width: Height:

Image Dimensions
Units Drop-Down
List Box

Picture 4.3: Upload Map Image Screen

- To submit a new image, click the [Browse] button on the right side of the **Image of facility location** text box. The **Choose file** dialog box will appear, where you will select the facility image file you would like to submit.

- When submitting a new image, you will need to specify the dimension units (in terms of width and height) of the image. From the **Image dimensions units** drop-down list box, you can select one of the following units of measurement: miles, meters, yards, feet, and decimal degrees. After selecting the measurement unit, provide the measurements in the **Width** and **Height** text boxes.
- When you are finished, click the [Upload map information] button. Click the [Cancel] button to leave the screen *without* uploading a new facility image file.

4.4 Tier 4 Status and Alternate Security Program Submission

CFATS provides Tier 4 facilities with the option of submitting a SVA or submitting an ASP in place of a SVA. After completing the **Facility Map** screen, all Tier 4 facilities will be directed to another screen which will provide the option to upload an ASP. All other facilities (e.g., Tier 1, Tier 2 and Tier 3) will be directed to the **Facility Security Issues** section to complete a CSAT SVA (see Section 5 for more details).

Before deciding whether to proceed with that option, a Tier 4 facility should be familiar with the requirements of 6 CFR §§ 27.215 and 27.235. Tier 4 facilities that choose to upload an ASP must also provide in the ASP the name of any (non-CSAT) SVA methodology previously used and the date the non-CSAT SVA was completed.

The following table lists the questions that must be answered to submit an ASP, as well as details regarding how the questions should be answered. Each of these questions requires Yes or No answers. If you answer *No* to any of these questions, you will be given the option of returning to the CSAT SVA (beginning with the **Facility Security Issues** section) or continuing with the ASP questions and the ASP uploading procedure.

Question #	ASP Question	Question Details
[Q:1.01-3315]	Do you want to upload an Alternate Security Program (ASP)?	• If you plan to upload an ASP and not complete the CSAT SVA, answer <i>Yes</i>, and follow the remaining instructions on uploading an ASP to DHS. • If you do not plan to upload an ASP, answer <i>No</i>, and you will be prompted to complete the CSAT SVA.

CSAT Security Vulnerability Assessment Application Instructions

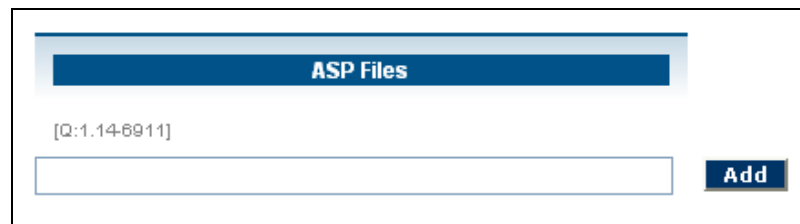
Question #	ASP Question	Question Details
[Q:1.1-3316]	SVA Scope (Issues and Chemicals of Interest): Does the ASP cover all of the facility assets that are associated with the security issues and chemicals of interest specified in the DHS Initial Notification letter?	When you answer Yes to this question, it is confirming that the ASP covers all COI above the threshold quantities detailed in Appendix A to CFATS, as well as all applicable security issues identified in the initial notification letter: • Release of toxic, flammable or explosive COI • Theft/diversion of COI • Sabotage/contamination of a COI.
[Q:1.1-11671]	Does the ASP use a Center for Chemical Process Safety (CCPS)-approved methodology?	Provide a Yes or No answer accordingly.
[Q:1.1-11672]	Does the ASP address the asset characterization factors described in 6 CFR 27.215?	Asset characterization includes: • The identification and characterization of potential critical assets; • The identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and • The identification of existing layers of protection.
[Q:1.1-11673]	Does the ASP address the threat assessment factors described in 6 CFR 27.215?	Threat assessment includes a description of possible internal threats, external threats, and internally-assisted threats.
[Q:1.1-3317]	Does the ASP cover all of the applicable attack modes included in the CSAT SVA?	When you answer Yes to this question, you are confirming that the ASP covers all applicable attack scenarios described in the CSAT SVA Attack Scenario Descriptions. The CSAT SVA Attack Scenario Descriptions are located online at csat.dhs.gov/csatsat, and are available to active CSAT users who have completed CVI training and have started their SVA. The descriptions cover the following threat areas: • Vehicle Borne Improvised Explosive Device (VBIED) • Maritime • Aircraft • Theft • Diversion • Sabotage • Assault Team • Standoff.

CSAT Security Vulnerability Assessment Application Instructions

Question #		
[Q:1.1-11674]	Does the ASP address the countermeasures factors described in 6 CFR 27.215?	Security vulnerability analysis includes the identification of potential security vulnerabilities and existing countermeasures, including their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards (RBPS).
[Q:1.1-11675]	Does the ASP address the risk assessment factors described in 6 CFR 27.215?	Risk assessment includes a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and a likelihood estimation of an attack's success.
[Q:1.13-3320]	Non-CSAT Security Vulnerability Assessment Methodology.	In the text box provided for this question, enter the name of the non-CSAT SVA methodology was previously used at the facility.
[Q:1.13-3331]	Date of Non-CSAT Security Vulnerability Assessment.	Enter the date of when the non-CSAT SVA methodology was used at the facility. Use the mm/dd/yyyy date format (e.g., May 1, 2006 is entered as 05/01/2006).

4.4.1 Uploading Alternate Security Program Documents

After you answer the previous questions, you will be prompted to submit ASP documents. Enter the name of the first ASP document you wish to submit in the text box provided, and then click the [Add] button next to it (see Picture 4.4).



ASP Files

[Q:1.14-6911]

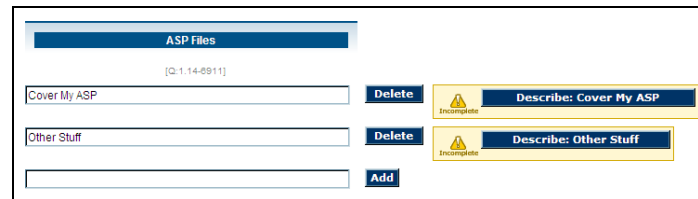
Add

Picture 4.4: ASP Document Name Text Box

CSAT Security Vulnerability Assessment Application Instructions

After the first document name is added, the following changes will happen to the screen:

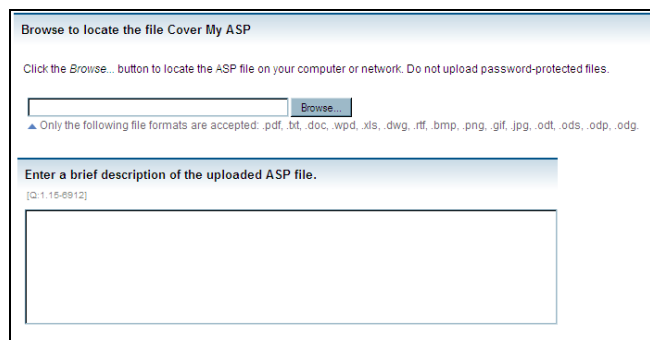
- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that document from your submission.
- Another text box and [Add] button will appear that will allow you to add additional documents. You can submit as many documents as needed.
- A [Describe] button will appear to the right of the text box where you entered the file name.



The screenshot shows a section titled "ASP Files". Below the title, there is a text input field containing "Cover My ASP" and a "Delete" button to its right. Below this, there is another text input field containing "Other Stuff" and a "Delete" button to its right. At the bottom of the section, there is an "Add" button. To the right of the "Delete" buttons, there are two yellow boxes with a warning icon and the text "Describe: Cover My ASP" and "Describe: Other Stuff" respectively.

Picture 4.5: ASP Document Delete and Describe Buttons

To submit a file with the document name, click the [Describe] button. The following screen will appear:



The screenshot shows a form titled "Browse to locate the file Cover My ASP". Below the title, there is a text input field and a "Browse..." button to its right. Below the input field, there is a message: "Click the Browse... button to locate the ASP file on your computer or network. Do not upload password-protected files." Below this, there is a list of accepted file formats: ".pdf, .txt, .doc, .wpd, .xls, .dwg, .rtf, .bmp, .png, .gif, .jpg, .odt, .ods, .odp, .odg". Below the list, there is a section titled "Enter a brief description of the uploaded ASP file." with a text input field.

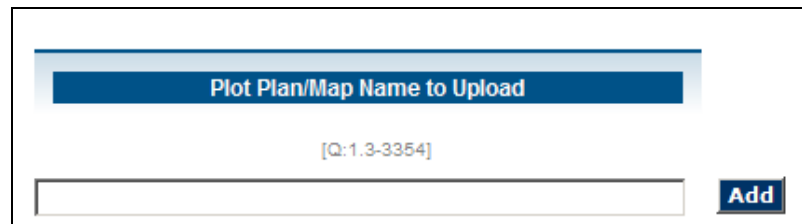
Picture 4.6: ASP Document Selection and Description Screen

Click the [Browse] button on the new screen. The **Choose file** dialog box will appear, where you will select from your computer or network the ASP document you would like to submit. In the text box provided below, enter a description of the file you are submitting. When you are finished, click the [Next] button at the bottom of the screen and you will be returned to the ASP document submission list screen.

When you are finished naming, uploading, and describing ASP documents, answer Yes to the question “Have you uploaded all ASP documents and provided detail information?”, which is located beneath your list of ASP documents, and click the [Next] button. You will be taken to the next screen in the ASP process.

4.4.2 Uploading Plot Plans/Maps

After you upload your ASP documents, you will be prompted to submit plot plans and/or maps for your facility site. Please be sure that the locations of assets that are analyzed in the submitted ASP for each COI and security issue are marked on the plot plans/maps. If necessary, include within the map a legend to icons/assets that are used in the plot plans/maps. Enter the name of the first plot plan/map you wish to submit in the text box provided, and then click the [Add] button next to it (see Picture 4.7).

The image shows a web form element. At the top is a blue header bar with the text "Plot Plan/Map Name to Upload" in white. Below this is a light blue rectangular area containing a text input field. Inside the input field, the text "[Q:1.3-3354]" is visible. To the right of the input field is a small blue button with the word "Add" in white.

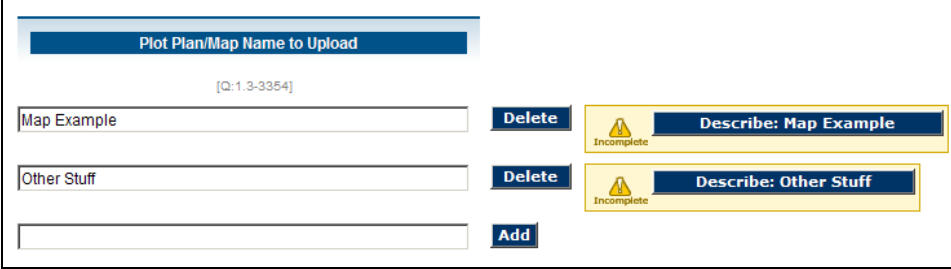
Picture 4.7: Plot Plan/Map Name Text Box

After the plot plan/map name is added, the following changes will happen to the screen:

- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that plot plan/map from your submission.
- Another text box and [Add] button will appear that will allow you to add additional plot plans/maps. You can submit as many plot plans/maps as needed.

CSAT Security Vulnerability Assessment Application Instructions

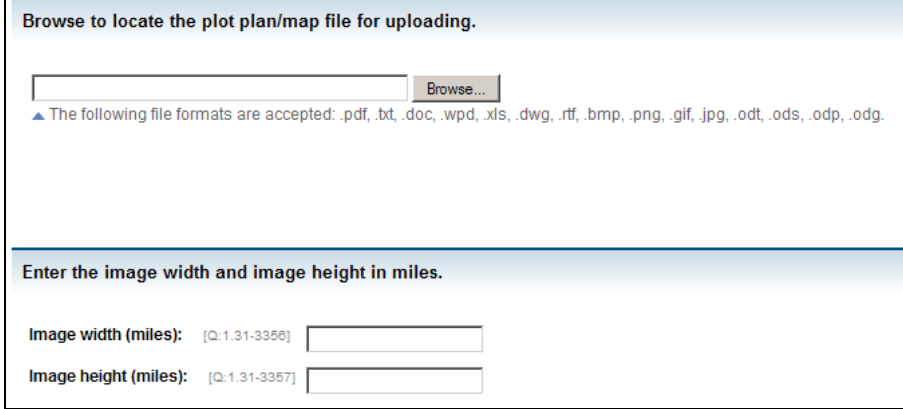
- A [Describe] button will appear to the right of the text box where you entered the file name.



The screenshot shows a form titled "Plot Plan/Map Name to Upload". Below the title is a reference code "[Q:1.3-3354]". There are three input fields for names: "Map Example", "Other Stuff", and an empty field. Each input field has a "Delete" button to its right. To the right of the "Map Example" and "Other Stuff" fields are "Describe" buttons, each preceded by a yellow warning icon and the word "Incomplete". At the bottom right of the form is an "Add" button.

Picture 4.8: Plot Plan/Map Name Delete and Describe Buttons

To submit a file with the plot plan/map name, click the [Describe] button. The following screen will appear:



The screenshot shows a form titled "Browse to locate the plot plan/map file for uploading." It features a text input field and a "Browse..." button. Below this is a message: "▲ The following file formats are accepted: .pdf, .txt, .doc, .wpd, .xls, .dwg, .rtf, .bmp, .png, .gif, .jpg, .odt, .ods, .odp, .odg." The second section of the form is titled "Enter the image width and image height in miles." and contains two rows: "Image width (miles): [Q:1.31-3356]" and "Image height (miles): [Q:1.31-3357]", each followed by a text input field.

Picture 4.9: Plot Plan/Map Selection and Description Screen

Click the [Browse] button on the new screen. The **Choose file** dialog box will appear, where you will select from your computer or network the plot plan/map you would like to submit. For each map image, provide the height and width dimensions in miles for the site depicted on the map in **Image width (miles)** and **Image height (miles)** text boxes provided below. When you are finished, click the [Next] button at the bottom of the screen and you will be returned to the plot plan/map submission list screen.

When you are finished naming, uploading, and describing plot plans/maps, answer Yes to the question “Have you uploaded all ASP documents and provided detail information?”, which is located beneath your list of plot plans/maps. You will then click the [Next] button to complete the ASP process.

4.4.3 Completing Alternate Security Program Submission

After completing the upload of ASP documents and plot plans/maps, the last screen in the ASP process will read: “Thank you for submitting an ASP for consideration by DHS. DHS will review your ASP submission and subsequently inform you of its acceptance or rejection.”

Click the [Next] button at the bottom of the screen to proceed. Instructions on final validation and final submission of your ASP are detailed in Section 9.

5. Facility Security Issues

The first step of the CSAT SVA process is to define the security issues and COI for the facility. The information that you enter into the **Facility Security Issues** section will enable you to define assets later in the **Asset Characterization** section. It will also serve as the basis for identifying the applicable attack scenarios in the **Vulnerability Analysis** section. To complete this section, you should refer to the DHS initial notification letter that identifies the facility's security issue(s) and the related COI.

5.1 Reporting Facility Security Issues

When completing the CSAT Top-Screen, the facility answered a number of questions pertaining to different security issues. Based on the facility's responses to the Top-Screen, none, some, or all of these security issues may be identified in the DHS initial notification letter. **NOTE:** Only the identified security issues documented by DHS in this letter must be entered into the CSAT SVA. The security issues that may be listed in a facility's DHS initial notification letter 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 weapon/chemical weapon convention precursor) chemicals; and/or
- Sabotage/contamination chemicals.

When the **Facility Security Issues** section of CSAT SVA is selected (either from the navigation bar or following the completion of information in the **General** section), you will need to answer seven questions. These questions require you to identify which security issues were reported by DHS in the initial notification letter. The following table lists the security questions that must be answered; each question requires a Yes or No answer.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question
[Q:2.0-971]	Release-Toxic COI: Does the DHS initial notification letter indicate that the facility should address security issues related to release-toxic COI?
[Q:2.0-3131]	Release-Flammable COI: Does the DHS initial notification letter indicate that the facility should address security issues related to release-flammable COI?
[Q:2.0-3132]	Release-Explosive COI: Does the DHS initial notification letter indicate that the facility should address security issues related to release-explosive COI?
[Q:2.0-3172]	Theft/Diversion-Explosive/Improvised Explosive Device Precursor COI: Does the DHS initial notification letter indicate that the facility should address security issues related to theft-EXP/IEDP COI?
[Q:2.0-3171]	Theft/Diversion-Weapons of Mass Effect COI: Does the DHS initial notification letter indicate that the facility should address security issues related to theft-WME COI?
[Q:2.0-3151]	Theft/Diversion-CW/CWP COI: Does the DHS initial notification letter indicate that the facility should address security issues related to theft-CW/CWP COI?
[Q:2.0-3173]	Sabotage/Contamination COI: Does the DHS initial notification letter indicate that the facility should address security issues related to sabotage/contamination COI?

NOTE: For some facilities, this information may be pre-populated. If the SVA has been pre-populated, the **Summary of COI and Security Issues** screen (see Picture 5.2) will be displayed, see section 5.3.

5.2 Reporting Chemicals of Interest

After you identify which security issues were reported by DHS in the initial notification letter, you will be required to identify the COIs that were reported by DHS in the initial notification letter on a screen similar to that in Picture 5.1.

Facility Security Information

« Back Next »

Release Toxic Chemicals of Interest

Indicate which release toxic chemicals of interest are listed in the DHS Initial Notification Letter.

The default settings on this list indicate that the chemical of interest is NOT listed in the letter. You must select Yes if the chemical is listed in the letter.

Chemical Name	CAS#	Was the chemical listed in the letter?
Acrolein [2-Propenal or Acrylaldehyde]	107-02-8	☒ Yes ☐ No
Allyl alcohol [2-Propen-1-ol]	107-18-6	☐ Yes ☒ No
Ammonia (anhydrous)	7664-41-7	☐ Yes ☒ No
Ammonia (conc. 20% or greater)	7664-41-7	☐ Yes ☒ No

[Q 2.1-1037]

Picture 5.1: COI Identification Screen

Depending on the number of security issues reported for your facility, up to six additional screens will be displayed for you to report the specific COIs related to those security issues and identified in the DHS initial notification letter. **NOTE:** These are the COIs and the security issues that will be the focus of the CSAT SVA.

For each security issue/chemical combination, you must select the COI identified under each security issue in the DHS initial notification letter. Each combination is listed in the following table.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:2.1-1037]	Release-Toxic COI	Select the release-toxic COI listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. You must change the answer to Yes for each chemical listed in the letter under the security issue Release of Toxic Chemicals .
[Q:2.2-1038]	Release-Flammable COI	Select the release-flammable COI that are listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. You must change the answer to Yes for each chemical listed in the letter under the security issue Release-Flammable Chemicals .
[Q:2.3-1039]	Release-Explosive COI	Select the release-explosive COI that are listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. You must change the answer to Yes for each chemical listed in the letter under the security issue Release-Explosive Chemicals .
[Q:2.6-1043]	Theft/Diversion-Explosive/IED Precursor COI	Select the theft/diversion-explosive/IED precursor COI that are listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. You must change the answer to Yes for each chemical listed in the letter under the security issue Theft/Diversion-Explosive/IED Precursor Chemicals .
[Q:2.5-1042]	Theft/Diversion-WME COI	Select the theft/diversion-WME COI that are listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. You must change the answer to Yes for each chemical listed in the letter under the security issue Theft/Diversion-WME Chemicals .
[Q:2.4-1041]	Theft/Diversion-CW/CWP COI	Select the theft/diversion-CW/CWP COI that are listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. The user must change the answer to Yes for each chemical listed in the letter under the security issue Theft/Diversion-CW/CWP Chemicals .
[Q:2.7-1671]	Sabotage/Contamination COI	Select the sabotage/contamination COI that are listed in the initial notification letter. The default settings for this question indicate that the chemicals are not present at the facility. The user must change the answer to Yes for each chemical listed in the letter under the security issue Sabotage/Contamination Chemicals .

5.3 Summary of Facility Security Issues

After you have indicated all of the COIs included in the DHS initial notification letter, a summary screen is shown (as seen below in Picture 5.2) that lists the COIs that you indicated were in the letter.

The screenshot shows a web application interface titled "Facility Security Information". At the top, there are navigation buttons: "<< Back" and "Next >>". Below this is a header section: "Summary of Chemical(s) of Interest and Security Issues Included in the Initial Notification Letter". The main content is divided into three sections, each with a light blue header:

- Release Toxic Chemicals of Interest**: Contains a table with two columns, "Chemical Name" and "CAS#".

Chemical Name	CAS#
Acrolein [2-Propenal or Acrylaldehyde]	107-02-8
- Release Flammable Chemicals of Interest**: Contains a table with two columns, "Chemical Name" and "CAS#".

Chemical Name	CAS#
Propylene [1-Propene]	115-07-1
- Release Explosive Chemicals of Interest**: Contains the text "No explosive chemicals of interest are present."

Picture 5.2: COI and Security Issues Summary Screen

If the information on the summary screen matches all of the security issues and COI from the DHS initial notification letter, select Yes and then click the [Next] button at the bottom of the screen to continue.

5.4 Facility Characteristics

For facilities that have Release-Toxic COIs, the following question must be answered:

Question #	SVA Question	Question Details
[Q:2.92-5911]	Facility Topography: What is the surrounding topography of the facility?	Select the option that best defines the area surrounding the facility: <i>Urban</i> or <i>Rural</i> . The entry here should match the corresponding entry in the CSAT Top-Screen. As in the Top-Screen, if a facility is covered by the EPA RMP rule (40 CFR Part 68), your answer should be consistent with the facility's current RMP on file with EPA. If a facility is not covered by a current RMP and the terrain surrounding the facility varies depending on the approach to the facility, select the topography (urban or rural) that is most representative of the facility's location. If you are still unsure, select <i>Rural</i> .

All facilities must answer the following question:

Question #	SVA Question	Question Details
[Q:2.92-3313]	Is the facility located on a navigable waterway?	You should answer <i>Yes</i> to this question if there is a waterway along any portion of the facility perimeter that can accommodate small-to-large watercraft. This includes vessels ranging between small pleasure craft, barges, and deep draft vessels. If you answer <i>No</i> for your facility, you will not evaluate a Maritime attack mode as part of the vulnerability analysis because it is not applicable for your facility.

5.5 Facility Security Information

When entering facility security information, you will need to enter information about security equipment, systems, inventory, and personnel controls.

5.5.1 Facility Security Equipment

If your facility has any security equipment that helps reduce the vulnerability of COI that the DHS initial notification letter has noted, select Yes on the top of the **Security Equipment** screen and answer the additional questions on the screen. If your facility does **not** have any security equipment to help reduce the vulnerability of COIs, select No and click the [Next] button on the bottom of the screen.

List any security equipment at the facility that might help reduce the vulnerability of COI. List only security equipment that applies across the entire facility, as opposed to equipment related to a specific COI or asset. Possible examples of security equipment include:

- Closed circuit TV (CCTV) surveillance systems
- Security response team and equipment location(s)
- Intrusion detection/monitored security alarm systems
- Security communications systems
- Other similar equipment or systems identified by the facility.

Security Equipment	Location	Support Systems Required
[Q.2.93-8331]	[Q.2.93-8332]	[Q.2.93-8333]
		Add

Picture 5.3: Facility Security Equipment Columns

Follow these steps when entering information on the **Security Equipment** screen:

1. Use the drop-down list box under the **Security Equipment** heading to select the name of the security equipment. **NOTE:** If the facility has none of the security equipment shown in the **Security Equipment** drop-down list box, leave this question blank and proceed to the question on the bottom of the screen, as listed in step 5.
2. Enter the location of the equipment in the text box under the **Location** heading.
3. Enter any support systems required to run the equipment in the text box under the **Support Systems Required** heading.
4. When you are finished entering information, click the [Add] button. A new entry line will appear for additional security equipment. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
5. If there are other types of security equipment at the facility that are not included in the drop-down box, answer Yes to the question at the bottom of the screen that reads, "Does the facility have other types of security equipment?" See Section 5.5.2 for more details. Click the [Next] button to continue.

Possible examples of information related to security equipment are described in the table below.

Equipment	Location	Support Systems Required
CCTV surveillance equipment covering all normal access points and major storage areas	Cameras are pole mounted and video system is monitored from the security station at the front gate	Electric power; system is not included on the emergency power backup system
Intrusion monitoring system (IMS) on all gates when they are not staffed by security personnel	Three gates, with intrusion notification to security station at front gate and corporate security center	Electric power; IMS is backed up for 45 minutes by UPS and can be switched to emergency AC power
Security guard vehicles and response equipment	Garaged next to onsite fire department at west end of plant	None
Emergency communications system within facility and to offsite responders	Security station at front gate	Normally provided with AC power, but operates on battery backup for up to 12 hours

CSAT Security Vulnerability Assessment Application Instructions

Equipment	Location	Support Systems Required
Perimeter fence line at 7 ft height, 2-inch 9-gauge chain-link mesh with 3-strand barb-wire outrigger/pedestrian and vehicle gates are commensurate in height and design with the fence line	Entire plant perimeter	None
Concrete jersey-type vehicle barriers	Positioned outside fence line near toxic COI rail car unloading station near the south perimeter fence line	None
Proximity Card Access Control System located at main vehicle gate grants access to plant employees to enter the site	Main gate on the north side of the site	Electric power; system is included on the emergency power backup system

5.5.2 Additional Security Equipment

If you answered Yes to the question “Does the facility have other types of security equipment?”, you will be taken to a screen with three columns, as seen in Picture 5.4.

Security Equipment Description	Location	Support Systems Required
[Q:2.931-8693]	[Q:2.931-8694]	[Q:2.931-8695]
		Add

Picture 5.4: Additional Facility Security Equipment Columns

CSAT Security Vulnerability Assessment Application Instructions

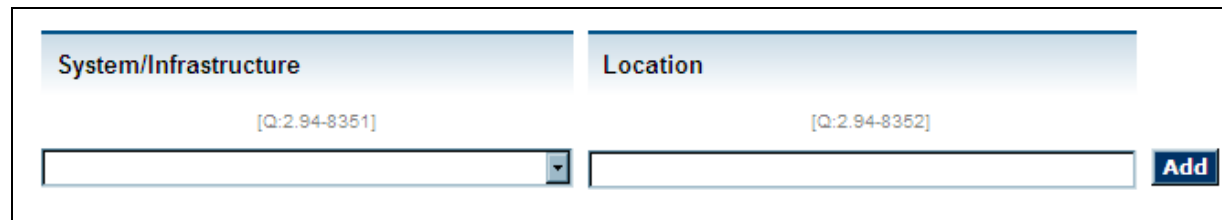
1. Use the text box under the **Security Equipment Description** heading to name and describe security equipment that you were not able to submit on the previous screen. List only security equipment that applies across the entire facility, as opposed to equipment related to a specific COI or asset.
2. Enter the location of the equipment in the text box under the **Location** heading.
3. Enter any support systems required to run the equipment in the text box under the **Support Systems Required** heading.
4. When you are finished entering information, click the [Add] button. A new entry line will appear for additional security equipment. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
5. When you are finished entering additional facility security equipment information, enter the appropriate answer to the question at the bottom of the screen, "Have all other security equipment been entered?" Click the [Next] button to continue.

5.5.3 Utility Systems and Infrastructure Support

If the facility has any utility systems or infrastructure support required for the security equipment, select Yes on the top of the **Utility Systems and Infrastructure Support** screen and answer the additional questions on the screen. If the facility does **not** have any utility systems or infrastructure support required for the security equipment, select *No* and click the [Next] button on the bottom of the screen.

List utility systems or other infrastructure support required by the security equipment and specify where on the facility the utility systems or infrastructure support are located. Possible examples include:

- Electric power systems
- Backup power systems
- Others identified by the facility.



System/Infrastructure	Location
[Q:2.94-8351]	[Q:2.94-8352]

Picture 5.5: Utility Systems and Infrastructure Support Columns

Follow these steps when entering information on the **Utility Systems and Infrastructure Support** screen:

1. Use the drop-down list box under the **System/Infrastructure** heading to select the name of the utility systems or infrastructure support. **NOTE:** If the facility has none of the utility systems or infrastructure support shown in the **Security Equipment** drop-down list box, leave this question blank and proceed to the question on the bottom of the screen, as listed in step 4.
2. Enter the location of the utility systems or infrastructure support in the text box under the **Location** heading.

3. When you are finished entering information, click the [Add] button. A new entry line will appear for additional utility systems or infrastructure support. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
4. If there are other types of utility systems or infrastructure support at the facility that are not included in the drop-down box, answer Yes to the question at the bottom of the screen that reads, “Does the facility have other types of utility systems or infrastructure?” See Section 5.5.4 for more details. Click the [Next] button to continue.

Possible examples of information related to utility systems or infrastructure support are described in the table below.

System/Infrastructure	Location
Electric power	Two offsite feeds to facility with redundant buses on site. UPS backup for instrumentation located in rack room at the Central Control Room. Emergency diesel backup power for critical safety loads located just west of control room.

5.5.4 Additional Utility Systems

If you answered Yes to the question “Does the facility have other types of utility systems or infrastructure?”, you will be taken to a screen with two columns, as seen in Picture 5.6.

The screenshot shows a web form with two columns. The left column is titled 'System/Infrastructure Description' and the right column is titled 'Location'. Both columns have a text input field with a placeholder text '[Q:2.941-8698]'. Below the input fields is a blue 'Add' button.

Picture 5.6: Additional Utility Systems and Infrastructure Support Columns

1. Use the text box under the **Security/Infrastructure Description** heading to name and describe utility systems or infrastructure support that you were not able to submit on the previous screen.
2. Enter the location of the equipment in the text box under the **Location** heading.
3. When you are finished entering information, click the [Add] button. A new entry line will appear for additional utility systems or infrastructure support. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
4. When you are finished entering additional facility security equipment information, enter the appropriate answer to the question at the bottom of the screen, "Have all other utility systems been entered?" Click the [Next] button to continue.

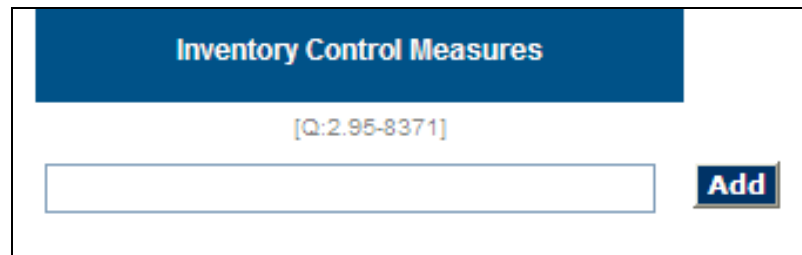
5.5.5 Inventory Control Measures

Facilities that have theft/diversion COI (as listed on the facility's DHS initial notification letter) will need to answer the following questions.

If the facility has any inventory control measures that would help reduce vulnerability to theft/diversion of COI, select Yes on the top of the **Inventory Control** screen and answer the additional questions on the screen. If the facility does **not** have any inventory control measures that would help reduce vulnerability to theft/diversion, select *No* and click the [Next] button on the bottom of the screen. Possible examples of information related to inventory control measures are described in the table below.

Inventory Control Measure	Automated?	Frequency Applied	Location	COI Covered
Electronic scanning of all specialty product inventory	Yes	Weekly	Storage area #7 and #8	Diborane
Packaged products are stored and inventoried separately	No	Weekly	Warehouse #10	Phosphine

Enter the name of the first inventory control measure you wish to submit in the text box provided on the **Inventory Control** screen, and then click the [Add] button next to it (see Picture 5.7).

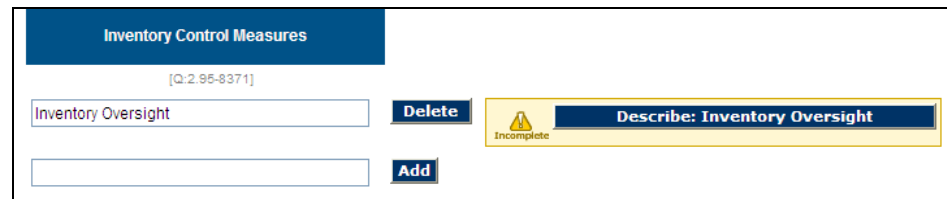


The screenshot shows a web interface titled "Inventory Control Measures" in a blue header. Below the header, there is a text input field containing the placeholder text "[Q:2.95-8371]". To the right of the text box is a blue button with the word "Add" in white text.

Picture 5.7: Inventory Control Measures Text Box

After you add the first inventory control measure, the following changes will happen to the screen:

- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that inventory control measure from your submission.
- Another text box and [Add] button will appear the first that will allow you to add additional inventory control measures. You can submit as many inventory control measures as needed.
- A [Describe] button will appear to the right of the text box where you entered the inventory control measure's name.



The screenshot shows the updated web interface. The "Inventory Control Measures" header is still present. Below it, the text input field now contains the text "Inventory Oversight". To the right of this text box is a blue button labeled "Delete". Below the first text box is a second, empty text input field. To the right of the second text box is a blue button labeled "Add". To the right of the "Delete" button is a yellow button with a warning icon and the text "Describe: Inventory Oversight".

Picture 5.8: Inventory Control Measures Delete and Describe Buttons

To submit a detailed description of the inventory control measure, click the [Describe] button. A new screen will appear which will require you to provide details regarding the following questions:

Question #	SVA Question	Question Details
[Q:2.951-8711]	Is the inventory measure automated?	Provide a Yes or No answer to this question.
[Q: 2.951-8372]	Frequency Applied	Use the drop-down list box to indicate the frequency with which the inventory control measure is applied.
[Q: 2.951-8373]	Location	Enter the location of the inventory control measure in the text box provided.
[Q: 2.951-10451]	Inventory Control Feature: Is the feature used in this control measure?	Identify features of the inventory control measure by providing a Yes or No answer for each of the inventory control features that are listed. Identify all that apply.
[Q:2.951-8511], [Q:2.951-8571], [Q:2.951-8573]	Chemicals Covered by the Measure	Identify any COI that are covered by the inventory control measure by providing a Yes or No answer for each of the Theft/Diversion COI that are listed. Identify all that apply.

When you are finished answering all of the inventory control measure description questions, select the Yes checkbox for the question “Have all inventory control measures used at the facility been entered?” at the bottom of the screen, and then click the [Next] button to continue.

When you are finished naming and describing inventory control measures, answer Yes to the question “Have all of the inventory control measures used at the facility that would help reduce vulnerability to theft/diversion been entered?”, which is located beneath your list of inventory control measures at the bottom of the **Inventory Control** screen. You will then click the [Next] button to continue.

5.5.6 Personnel Access Control Measures

If the facility has any personnel access control measures that would help reduce vulnerability to an attack, select Yes on the top of the **Personnel Access Control Measures** screen and answer the additional questions on the screen. If the facility does **not** have any personnel access control measures that would help reduce vulnerability to an attack, select No and click the [Next] button on the bottom of the screen.

List any personnel access control systems in place at the facility that would be considered useful in reducing vulnerability to an attack. Possible examples include:

- Verification of credentials for all employees and visitors before entering the facility.
- Allowing only authorized staff and vetted, escorted visitors to buildings at, near or adjacent to the facility's assets.

Access Control Measure	Is the control measure automated?	Frequency Applied	Location	Personnel Covered	
[Q:2.96-8431]	[Q:2.96-8712]	[Q:2.96-8432]	[Q:2.96-8433]	[Q:2.96-8434]	
	☐ Yes ☐ No				Add

Picture 5.9: Personnel Access Control Measures Columns

Follow these steps when entering information on the **Personnel Access Control Measures** screen:

1. Use the drop-down list box under the **Access Control Measure** heading to select the name of the measure. The list options include:
 - **Personnel recognition by officer:** Access control system based on personnel recognition by security officer with no picture or electronic badge.
 - **Manual badge validation by officer:** Access control system with manual badge validation by security officer.
 - **Biometric validation:** Access control system with biometric validation.
 - **Computerized access with no validation:** Access control system with computerized access with no validation (e.g., swipe or proximity card system with no guard or computer validation process).
 - **Personnel access allowed on foot only:** Personnel access allowed on foot only (i.e., employee and visitor vehicles not allowed inside facility process boundary).

NOTE: If the facility has none of the personnel access control measures shown in the **Access Control Measure** drop-down list box, leave this question blank and proceed to the question on the bottom of the screen, as listed in step 7.

2. Enter the appropriate *Yes* or *No* answer under the **Is the control measure automated?** heading.
3. Use the drop-down list under the **Frequency Applied** heading to indicate the frequency with which the measure is applied.
4. Enter the location of the access control measure in the text box under the **Location** heading.
5. Enter the personnel who are covered by the access control measure in the text box under the **Personnel Covered** heading.
6. When you are finished entering information, click the [Add] button. A new entry line will appear for additional personnel access control measures. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
7. If there are other types of personnel access control measures at the facility that are not included in the drop-down list box, answer *Yes* to the question at the bottom of the screen that reads, “Does the facility have other types of personnel access control measures?” See Section 5.5.7 for more details. Click the [Next] button to continue.

Possible examples of information related to personnel access control systems are described in the table below.

Personnel Access Control Measure	Automated?	Frequency Applied	Location	Personnel Covered
Badge swipe system	Yes	24 hours a day, 7 days a week	Front gate and all access points	All full/time and part time employees

5.5.7 Additional Personnel Access Controls

If you answered Yes to the question “Does the facility have other types of personnel access control measures?”, you will be taken to a screen with five columns, as seen in Picture 5.10.

Personnel Access Control Description	Is the control measure automated?	Frequency Applied	Location	Personnel Covered
[Q:2.961-8714]	[Q:2.961-8715]	[Q:2.961-8716]	[Q:2.961-8717]	[Q:2.961-8718]
	☐ Yes ☐ No			Add

Picture 5.10: Additional Personnel Access Control Measures Columns

1. Use the text box under the **Personnel Access Control Measure** heading to name and describe the personnel access control measure that you were not able to submit on the previous screen.
2. Enter the appropriate Yes or No answer under the **Is the control measure automated?** heading.
3. Use the drop-down list under the **Frequency Applied** heading to indicate the frequency with which the measure is applied.
4. Enter the location of the equipment in the text box under the **Location** heading.
5. Enter the personnel who are covered by the access control measure in the text box under the **Personnel Covered** heading.
6. When you are finished entering information, click the [Add] button. A new entry line will appear for additional personnel access control measures. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
7. When you are finished entering additional personnel access control measure information, enter the appropriate answer to the question at the bottom of the screen, “Have all other access control measures been entered?” Click the [Next] button to continue.

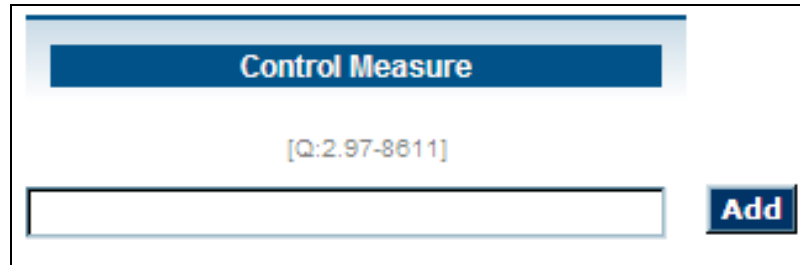
5.5.8 Shipping and Receiving Control Measures

Facilities that have theft/diversion or sabotage COI (as listed on the facility's DHS initial notification letter) will need to answer the following questions.

If there are any shipping and receiving control measures in place at the facility that would be considered useful in reducing vulnerability to an attack, select **Yes** on the top of the **Shipping and Receiving Control Measures** screen and answer the additional questions on the screen. If there are **no** shipping and receiving control measures in place at the facility that would be considered useful in reducing vulnerability to an attack, select **No** and click the [Next] button on the bottom of the screen. Possible examples of information related to shipping and receiving control measures are described in the table below.

Shipping and Receiving Control Measure	Automated?	Frequency Applied	Location	COI Covered
Inspection of delivery vehicles	No	Daily	2 shipping/receiving docks at the facility	Diborane

Enter the name of the first shipping and receiving control measure you wish to submit in the text box provided on the **Shipping and Receiving Control Measures** screen, and then click the [Add] button next to it (see Picture 5.11).

The image shows a software interface for adding control measures. It features a blue header bar with the text "Control Measure". Below the header is a text input field containing the placeholder text "[Q:2.97-8611]". To the right of the input field is a blue button with the text "Add".

Picture 5.11: Shipping and Receiving Control Measures Text Box

After you add the first shipping and receiving control measure, the following changes will happen to the screen:

- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that shipping and receiving control measure from your submission.
- Another text box and [Add] button will appear. The text box will allow you to add additional shipping and receiving control measures. You can submit as many shipping and receiving control measures as needed.
- A [Describe] button will appear to the right of the text box where you entered the control measure's name.



The screenshot displays a web application interface for managing control measures. At the top, there is a header bar labeled "Control Measure". Below this, a text input field contains the text "Shipping Control Measure". To the right of this field is a blue button labeled "Delete". Below the first text field is another empty text input field, and to its right is a blue button labeled "Add". To the right of the "Add" button is a yellow warning icon with the word "Incomplete" below it. Further to the right is a blue button labeled "Describe: Shipping Control Measure".

Picture 5.12: Shipping and Receiving Control Measures Delete and Describe Buttons

To submit a detailed description of the shipping and receiving control measure, click the [Describe] button. A new screen will appear which will require you to provide details regarding the following questions:

Question #	SVA Question	Question Details
[Q:2.971-8719]	Is the control measure automated?	Provide a Yes or No answer for this question.
[Q:2.971-8612]	Frequency Applied	Use the drop-down list box to indicate the frequency with which the control measure is applied.
[Q:2.971-8613]	Location	Enter the location of the control measure in the text box provided.
[Q:2.971-10012]	Control Measure Feature: Is the feature used in this control measure?	Identify features of the control measure by providing a Yes or No answer for each of the control features that are listed. Identify all that apply.
[Q:2.971-8659], [Q:2.971-8665], [Q:2.971-8666], [Q:2.971-8671]	Chemicals Covered by the Measure	Identify any COI that are covered by the control measure by selecting a Yes or No option button for each of the COI that are listed. Identify all that apply.

When you are finished answering all of the shipping and receiving control measure description questions, select the Yes check box for the question, “Has all appropriate information about the shipping and receiving control measure been completed?” at the bottom of the screen, and then click the [Next] button to continue.

When you are finished naming and describing shipping and receiving control measures, answer Yes to the question “Have all shipping and receiving control measures at the facility been entered?”, which is located beneath your list of shipping and receiving control measures at the bottom of the **Shipping and Receiving Control Measures** screen. You will then click the [Next] button to continue.

5.5.9 Post-Release Measures and Equipment

Facilities that have release toxic COI (as listed on the facility’s DHS initial notification letter) will need to answer the following questions.

If the facility has any post-release measures and/or equipment that would be considered useful in reducing the consequence of a toxic release, select Yes on the top of the **Post-Release Measures and Equipment** screen and answer the additional questions on the screen. If the facility does **not** have any post-release measures and/or equipment that would be considered useful in reducing the consequence of a toxic release, select *No* and click the [Next] button on the bottom of the screen.

List any post-release measures and/or equipment that would be considered useful in reducing the consequence of a toxic release. Do **not** list mitigation systems that only apply to a single asset (e.g., a secondary containment dike around toxic liquid storage). Possible examples of post-release measures and/or equipment include:

- Community emergency warning system: auto-dialer
- Community emergency warning system: sirens
- Others identified by the facility.

Post-Release Measures and Equipment	Location	Support Systems Required
[Q.2.98-8451]	[Q.2.98-8452]	[Q.2.98-8453]
		Add

Picture 5.13: Post-Release Measures and Equipment Columns

Follow these steps when entering information on the **Post-Release Measures and Equipment** screen:

1. Use the drop-down list box under the **Post-Release Measures and Equipment** heading to select the name of the post-release measure or equipment. **NOTE:** If the facility has none of the post-release measures or equipment shown in the **Post-Release Measures and Equipment** drop-down list box, leave this question blank and proceed to the question on the bottom of the screen, as listed in step 5.
2. Enter the location of the post-release measure or equipment in the text box under the **Location** heading.
3. Enter any support systems required to run the post-release measure or equipment in the text box under the **Support Systems Required** heading.

- When you are finished entering information, click the [Add] button. A new entry line will appear for additional post-release measures or equipment. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
- If there are other types of post-release measures or equipment at the facility that are not included in the drop-down box, answer Yes to the question at the bottom of the screen that reads, “Does the facility have other types of post-release measures?” See Section 5.5.10 for more details. Click the [Next] button to continue.

Possible examples of information related to post-release measures or equipment are described in the table below:

Measures/Equipment	Location	Support Systems Required
Community emergency notification system (auto-dialer system) – used in the event of a toxic release that might have offsite impacts	Messages initiated from onsite security station or emergency command center are distributed via county auto-dial system located at County Emergency Services Building	Normal or emergency communications system

5.5.10 Additional Post-Release Measures

If you answered Yes to the question “Does the facility have other types of post-release measures?”, you will be taken to a screen with three columns, as seen in Picture 5.14:

Post-Release Equipment/Application Description	Location	Support Systems Required
[Q:2.981-8721]	[Q:2.981-8722]	[Q:2.981-8723]
		Add

Picture 5.14: Additional Post-Release Measures and Equipment Columns

- Use the text box under the **Post-Release Equipment/Application Description** heading to name and describe the post-release measure or equipment that you were not able to submit on the previous screen.

2. Enter the location of the post-release measure or equipment in the text box under the **Location** heading.
3. Enter any support systems required to run the post-release measure or equipment in the text box under the **Support Systems Required** heading.
4. When you are finished entering information click the [Add] button. A new entry line will appear for additional post-release measures or equipment. Continue adding entries until all applicable items have been provided. After each entry the [Add] button will change to a [Delete] button that you can use if you choose to delete an entry from your submission.
5. When you are finished entering additional post-release measures and/or equipment information, enter the appropriate answer to the question at the bottom of the screen, "Have all other post-release measures been entered?" Click the [Next] button to continue.

5.5.11 Site Vulnerability Factors

If the facility has any features, offsite terrain, or infrastructure items that potentially increase the facility's vulnerability to attack, select **Yes** on the top of the **Site Vulnerability Factors** screen and answer the additional questions on the screen. If the facility does **not** have any features, offsite terrain, or infrastructure items that potentially increase the facility's vulnerability to attack, select **No** and click the [Next] button on the bottom of the screen.

List any facility features, offsite terrain, or infrastructure items that potentially increase the facility's vulnerability to attack. Possible examples of such attributes include:

- Limited physical access to the facility for emergency responders and law enforcement.
- Terrain or buildings that allow surveillance or aid attacks of the facility from outside the facility's boundaries.
- Other attributes identified by the facility.

Site Vulnerability	Comment
[Q:2.99-8454]	[Q:2.99-8455]
Add	

Picture 5.15: Site Vulnerability Factor Columns

Follow these steps when entering information on the **Site Vulnerability Factors** screen:

1. Use the text box under the **Site Vulnerability** heading to enter any facility features, offsite terrain, or infrastructure items that potentially increase the site's vulnerability to attack.
2. Enter a comment or description about the vulnerability in the text box under the **Comment** heading.
3. When you are finished entering information, click the [Add] button. A new entry line will appear for additional vulnerabilities. Continue adding entries until all applicable items have been provided. After each entry, the [Add] button will change to a [Delete] button, which you can use if you choose to delete an entry from your submission.
4. When you are finished entering all site vulnerabilities, enter the appropriate answer to the question at the bottom of the screen, "Have all site vulnerability factors been entered?" Click the [Next] button to continue.

Possible examples of information related to site vulnerabilities are described in the table below:

Site Vulnerability	Comments
Facility access for security or emergency response vehicles	The facility is accessible through one point of entry from a public road.
Electric power	All offsite power to the facility is provided via a single substation.
Railroad	A rail access line to other facilities passes through the facility property with gates controlled by the railroad, and no notification to the facility when the rail line is to be used for accessing the other facility.
Highway bridge	A portion of a U.S. highway bridge passes over the facility, so items can be dropped from the bridge inside the facility fence line and near specific storage areas.
Railroad access road and rail spur	The rail spur and rail company access road is located within 50 feet of the south fence line of the plant site.

6. Asset Characterization

The second step of the CSAT SVA process is to identify one or more assets that are associated with the COI and security issue(s) that were entered in the **Facility Security Issues** section of the SVA. The assets selected for analysis by a facility for the SVA will vary by:

- The quantity of COI,
- The security issues associated with the specific COI,
- The configuration of the equipment; and
- The potential vulnerability of the equipment, based on the equipment's location or other factors.

6.1 Identifying Assets

A "Primary COI" is the COI for which the consequences of damage to a particular facility asset will be estimated. The CSAT SVA is arranged so that each facility asset is associated with one Primary COI; thus, your facility must identify at least one asset for each COI included in the facility's DHS initial notification letter (i.e., each COI must be listed as a "primary" COI for at least one asset).

An asset that is associated with more than one COI might need to be identified multiple times, with each COI listed as the Primary COI for that asset. For example, if you have a building that houses both COI X and COI Y, then you would do the following:

1. Identify the building as Asset 1 and identify COI X as the Primary COI for Asset 1.
2. Identify the *same building* as Asset 2, but identify COI Y as the Primary COI for Asset 2.

The instructions in the following pages describe the criteria for identifying assets based on the type of COI. The instructions address asset characterization for each security issue that the COI presents (i.e., release, theft/diversion, or sabotage contamination). COI-related assets may include, but are not limited to:

- Vessels;
- Process units;
- Piping;
- Equipment items;

- Transportation packaging (or clusters of packages); or
- Other containers that hold a specific COI. For the purposes of these instructions, any hardware, packaging, or other containers holding a COI is referred to as “equipment.”

Assets are required for each identified combination of COI and security issue. If a single COI has more than one security issue associated with it (e.g., a COI included in the DHS initial notification letter raises two security issues: release and theft/diversion), the user should define a separate asset for each security issue. In most cases, these assets would be distinct equipment items (e.g., a bulk storage tank and a portable container). Yet in other cases, the assets might be the same equipment (e.g., a portable tank that contains an amount of COI that needs to be considered for release *and* for theft/diversion.)

The tables below outline the asset identification process in the context of particular security issues and COI.

Asset Identification Category	Asset Identification for Release COI
Asset Identification Description	Identify one or more assets for each Release COI (i.e., Release-Toxic, Release-Flammable, or Release-Explosive) included in the facility's DHS initial notification letter. Assets must be characterized for each Release COI.
Asset Identification Process	1. Identify the equipment at the facility that contains the largest inventory of the specific COI being considered as an asset. This could be a single item or multiple equipment items that contain the COI and are connected in such a way that severe damage to one of the equipment items could potentially result in the release of the inventory in all of them. 2. Identify additional equipment items, or a collection of connected equipment, as an asset if the equipment is associated with a COI inventory other than that identified in step 1 above and where the vulnerability of that asset to attack is expected to be greater than for the asset identified in step 1 above due to accessibility, configuration, ease of use by an adversary, and/or other factors. 3. Identify additional equipment items, or a collection of connected equipment, as an asset if the equipment is associated with a COI inventory other than that identified in step 1 above and where the consequences of an attack on the asset are expected to be different (e.g., involve other inventories of the COI located nearby or might affect areas offsite that are different from the areas affected by the asset identified in step 1 above). 4. If an equipment item contains the largest inventory of two different COI identified in the Facility Security Issues section, it should be treated as two separate assets (one for each COI).

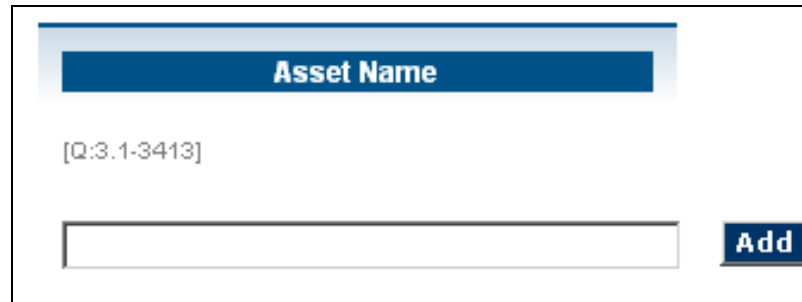
CSAT Security Vulnerability Assessment Application Instructions

Asset Identification Category	Asset Identification for Theft/Diversion COI
Asset Identification Description	Identify one or more assets for each Theft/Diversion COI included in the facility's DHS initial notification letter. When entering information for theft and/or diversion scenarios, a facility must identify assets that contain an amount at or above the Theft/Diversion Screening Threshold Quantity (STQ) for that COI, as specified in Appendix A to 6 CFR Part 27.
Asset Identification Process	1. Identify an asset with the largest quantity of the COI. As provided in 6 CFR § 27.203, DHS uses the definition of "transportation packaging" in 49 CFR § 171.8. This includes, but is not limited to, cylinders, bulk bags, bottles (inside or outside of a box), cargo tanks, and tank cars (detached from motive power). 2. Identify additional assets with smaller quantities of COI in transportation packaging where vulnerability to attack (theft or diversion) is expected to be greater than for the asset identified in step 1 above due to portability, availability, ease of use by an adversary, and/or other factors.

Asset Identification Category	Asset Identification for Sabotage/Contamination COI
Asset Identification Description	Identify one or more assets for each Sabotage/Contamination COI identified in the facility's DHS initial notification letter. When entering information for sabotage/contamination scenarios, the facility must identify assets that contain a quantity of a Sabotage/Contamination COI at or above the applicable Screening Threshold Quantity (STQ) for the COI, as specified in Appendix A to 6 CFR Part 27.
Asset Identification Process	1. Identify an asset with the largest amount of the Sabotage/Contamination COI that the facility ships and requires a placard under Department of Transportation (DOT) hazardous materials regulations (Subpart F of 49 CFR Part 172). 2. Identify additional assets with smaller amounts of Sabotage/Contamination COI that the facility ships and require a placard under DOT hazardous materials regulations (Subpart F of 49 CFR Part 172) where vulnerability to attack (contamination) is expected to be greater than for the asset identified in step 1 above due to availability, ease of use by an adversary, and/or other factors.

6.2 Characterizing Assets

On the first screen of the **Asset Characterization** section, you will be asked to identify a facility asset by entering its name on the text box provided and then click the [Add] button next to it (as seen in Picture 6.1).

The image shows a user interface for entering an asset name. At the top is a blue header bar with the text "Asset Name" in white. Below this is a text input field with a light blue border and a light blue background. Inside the input field, the text "[Q:3.1-3413]" is displayed in a small, grey font. To the right of the input field is a blue button with the word "Add" in white text.

Picture 6.1: Asset Name Text Box

The **Asset Name** text box can be up to 34 characters in length and contain a mix of alphanumeric data. The names should be distinct enough to identify the asset during the following screens. Examples of possible asset names, which include the equipment, primary COI, and/or the primary security issue, are listed in the table below:

Facility Name	Facility Asset Names
Facility ABC	- Asset 1: Bulk Storage Tank 1103-Chem X - Asset 2: Isotainer Tank-Area 1-Chem X - Asset 3: Isotainer Tank-Area 1-Diversion
Facility DEF	- Asset 1: Isotainer Tank-Unit 1-Rel. Toxic - Asset 2: Iso Tank-Material Receiving Area

After you add the first asset name, the following changes will happen to the screen:

- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that asset name from your submission.
- Another text box and [Add] button will appear the first that will allow you to add additional asset names. You can submit as many asset names as needed.
- A [Describe] button will appear to the right of the text box where you entered the asset name.

Asset Name	
[Q:3.1-3413] Tank 123 - Acrolein - Release	Delete Describe: Tank 123 - Acrolein - Release (Incomplete)
Tank 456 - Propylene - Release	Delete Describe: Tank 456 - Propylene - Release (Complete)
R&D Lab - Arsenic Trichloride - Theft/Diversior	Delete Describe: R&D Lab - Arsenic Trichloride - Theft/Diversior (Complete)

Picture 6.2: Asset Name Delete and Describe Buttons

To submit a detailed description of the asset you entered, click the [Describe] button. New screens will appear which will require you to provide details regarding the following questions:

Question #	SVA Question	Question Details
[Q:3.31-3831]	Enter a brief description of the asset.	Provide a brief description of the asset in the text box provided, including: • Its primary function (e.g., storage, production, loading/unloading); • The number and type of grouped or interconnected vessels; and • Any additional facility-identifying number or name.

Question #	SVA Question	Question Details
[Q:3.2-10211-10217]	Select only one primary security issue.	Each asset needs to have one primary security issue associated with it. The Primary COI will be determined from the Primary Security Issue. The Primary Security Issue is the security issue for which the vulnerability and consequence associated with attacks on the asset are estimated. If more than one security issue is associated with an asset, the asset should be considered as two separate assets and entered with two separate names. Likewise, if an asset contains the largest inventory of two different COI, it should be considered as two separate assets, one for each COI. Check one—and only one—primary security issue by using the check boxes provided.
[Q:3.31-12192]	Select the items below where the COI is located or contained within this asset.	Use the Yes and No option buttons to select the items where the COI is located or contained within the asset. Select all that apply.

6.2.1 Chemical of Interest Associated with an Asset

After identifying the items below where the COI is located or contained within the asset, you will need to identify the chemicals associated with the asset. All COI associated with the asset should be selected, regardless of whether they will be defined as the Primary COI for the asset. **NOTE:** Only the COI that you entered in the **Facility Security Issues** section will be available for selection.

Question #	SVA Question	Question Details
[Q:3.31-3473]	Select all Release-Toxic COI associated with this asset.	Any Release-Toxic COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.
[Q:3.31-3493]	Select all Release-Flammable COI associated with this asset.	Any Release-Flammable COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.
[Q:3.31-3500]	Select all Release-Explosive COI associated with this asset.	Any Release-Explosive COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.

Question #	SVA Question	Question Details
[Q:3.31-3520]	Select all Theft/Diversion-Explosive/Improvised Explosive Device Precursor (EXP/IEDP) COI associated with this asset.	Any Theft/Diversion-EXP/IEDP COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.
[Q:3.31-3514]	Select all Theft/Diversion-Weapons of Mass Effect (WME) COI associated with this asset.	Any Theft/Diversion-WME COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.
[Q:3.31-3507]	Select all Theft/Diversion-Chemical Weapon/Chemical Weapons Precursors (CW/CWP) COI associated with this asset.	Any Theft/Diversion-CW/CWP COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.
[Q:3.31-3527]	Select all Sabotage/Contamination COI associated with this asset.	Any Sabotage/Contamination COI identified in the Facility Security Issues section will be listed. Select any which are associated with this asset.

6.2.2 Detailed Asset Chemical of Interest Information

You will be asked a series of questions for each COI that has been identified at the asset, including which chemical is the Primary COI. When calculating the quantity of COI, use the same counting rules provided by CFATS for calculating the applicable STQs for chemicals of interest. Only screens for the identified chemicals will be shown; for example, if no Release-Toxic COI were indicated to be associated with the asset, the **Toxic Chemical** screen will not be shown.

NOTE: If the same physical structure is defined as an asset multiple times for multiple Primary COIs, you will need to enter the chemical information more than once. For example, Asset 1 has a Primary COI of chemical X, and the same physical structure is also defined as Asset 2 with Primary COI Y and a chemical Z is also physically present. The facility will answer the detailed questions about chemicals X, Y and Z for both Asset 1 and Asset 2.

The following sub-sections and tables will provide additional guidance for providing information for security issues and COIs.

6.2.2.1 Release-Toxic Chemical of Interest

- If you indicated that a Release-Toxic was the primary security issue, you will be asked to identify the primary COI and then provide detail information about each chemical at the asset.
- If you indicated that a Release-Toxic COI was associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each Release-Toxic COI at the asset.
- If **no** Release-Toxic COI is associated with the asset, you will **not** see the Release-Toxic COI screen.

Question #	SVA Question	Question Details
[Q:3.41-8851]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Release-Toxic COI. Select only one chemical as the Primary COI for the asset. Because only one chemical can be listed as the Primary COI, assets with multiple COIs that should be the Primary COI will need to be identified as multiple assets.
[Q:3.41-3475]	Quantity (pounds).	You are required to enter the total quantity, in pounds, of each Release-Toxic COI associated with the asset. Round the quantity to two significant digits (e.g., round 247500 pounds to 250000 pounds, and round 7625 pounds to 7600 pounds). Do not use commas when entering data. The quantity associated with the asset is the total quantity of that Release-Toxic COI within the equipment or collection of equipment items.
[Q:3.41-6993]	Select the predominant chemical phase of the chemical at this asset.	Use the drop-down list menu to select the predominant chemical phase of the chemical at this asset. For example, select <i>Liquid</i> for the predominant phase if the chemical is a liquid at or near atmospheric temperature and pressure.
[Q:3.41-8892]	Is the facility's largest inventory of the COI at this asset?	Answer Yes if the asset contains the largest inventory of the COI.

For Release-Toxic COIs that were listed as predominantly liquids at this asset, the following questions will be asked:

Question #	SVA Question	Question Details
[Q:3.412-6995]	Temperature (degree Fahrenheit)	Provide the correct temperature in the text box provided.
[Q:3.412-8893]	Process or storage pressure (psig)	Provide the correct process or storage pressure in the text box provided.
[Q:3.412-8894]	Liquid height (feet)	Enter the height of the liquid above the vessel bottom.
[Q:3.412-6996]	Is the liquid an aqueous solution?	Use the Yes and No option buttons to select the appropriate answer. <i>If the answer to this question is Yes, you will be directed to an additional question (see below).</i>
[Q:3.413-7011]	Percent Concentration by Weight	In the text box provided, enter the initial percent concentration by weight of the toxic chemical in aqueous solution associated with this asset.

For assets that have Release-Toxic as the primary security issue, enter any measures in place that you expect to help mitigate a toxic release. Check the box for each mitigation measure that is in place at the facility and is expected to be beneficial in a toxic release. At a later point in the SVA, you will be able to document whether these mitigation measures would be expected to survive an attack (see Section 7.4.5).

You will be able to choose from the following list of mitigation measures:

- Dike, berm, or other similar containment
- Leak detection system (e.g., fixed chemical detectors with alarm)
- Fixed vapor suppression system (e.g., foam or dry chemical cover, water spray system)
- Notification system for offsite evacuation or sheltering in place (e.g., phone dialing system, alarm system)
- Other measures.

If you selected any of the mitigation measures provided, you will be directed to screens to provide further details. If you did **not** select any of the mitigation measures, you will be directed to the next COI associated with the asset. The table below outlines the additional details you will have the option of providing for each mitigation measure.

Mitigation Measures and Question Numbers	Mitigation Measure Details and Question Numbers
Dike, berm, or other similar containment [Q:3.42-10471]	• Description of containment [Q:3.421-9211] • Containment area (sq ft) [Q:3.421-9212] • Containment capacity (gallons) [Q:3.421-9213]
Leak detection system [Q:3.42-10472]	• Description of system [Q:3.421-9214] • Estimated time to detection for a toxic release (minutes) [Q:3.421-9215]
Fixed vapor suppression system [Q:3.42-10473]	• Description of system [Q:3.421-9216] • Estimated time to activation for this scenario (minutes) [Q:3.421-9218] • Estimated vapor reduction for a toxic release (%) [Q:3.421-9219]
Notification system for offsite evacuation or sheltering in place [Q:3.42-10474]	• Description of system [Q:3.421-9220] • Estimated time to activation of system (minutes) [Q:3.421-9221] • Description of community outreach/training on evacuation and sheltering in place [Q:3.421-9222]
Other measures [Q:3.42-10475]	• Description of other measures [Q:3.421-9223] • Description of expected mitigation for a toxic release [Q:3.421-9224]

6.2.2.2 *Release-Flammable Chemical of Interest*

- If you indicate that a Release-Flammable COI is the primary security issue, you will be asked to identify the Primary COI and then provide detailed information about each chemical at the asset.
- If you indicate that a Release-Flammable COI is associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each Release-Flammable COI at the asset.

- If **no** Release-Flammable COI is associated with the asset, you will **not** see the Release-Flammable COI screen.

Question #	SVA Question	Question Details
[Q:3.43-8854]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Release-Flammable COI. Select only one chemical as the Primary COI for this asset. Since only one chemical can be listed as the Primary COI, assets with multiple COIs that should be the Primary COI will need to be defined as multiple assets.
[Q:3.43-3496]	Quantity (pounds) for each Release-Flammable COI at the asset.	You are required to enter the total quantity, in pounds, of each Release-Flammable COI associated with the asset. Round the quantity to two significant digits (e.g., round 247500 pounds to 250000 pounds, and round 7625 pounds to 7600 pounds). Do not use commas when entering data.
[Q:3.43-8971]	Is the facility's largest inventory of the COI at this asset?	Answer Yes if the asset contains the largest inventory of the COI.

6.2.2.3 Release-Explosive Chemical of Interest

- If you indicate that a Release-Explosive COI is the primary security issue, you will be asked to identify the Primary COI and then provide detailed information about each chemical at the asset.
- If you indicate that a Release-Explosive COI is associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each release-explosive COI at the asset.
- If **no** Release-Explosive COI is associated with the asset, you will **not** see the Release-Explosive COI screen.

Question #	SVA Question	Question Details
[Q:3.45-8856]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Release-Explosive COI. Select only one chemical as the Primary COI for this asset. Because only one chemical can be listed as the Primary COI, assets with multiple COIs that should be the Primary COI will need to be defined as multiple assets.

Question #	SVA Question	Question Details
[Q:3.45-3503]	Quantity (pounds) for each explosive COI at the asset.	You are required to enter the total quantity, in pounds, of each Release-Explosive COI associated with the asset. Round the quantity to two significant digits (e.g., round 247500 pounds to 250000 pounds, and round 7625 pounds to 7600 pounds). Do not use commas when entering data.
[Q:3.45-9005]	Is the facility's largest inventory of the COI at this asset?	Answer Yes if the asset contains the largest inventory of the COI.

6.2.2.4 Theft/Diversion-Explosive/IEDP COI

- If you indicate that a Theft/Diversion-Explosive/IEDP COI is the primary security issue, you will be asked to identify the Primary COI and then provide detailed information about each chemical at the asset.
- If you indicate that a Theft/Diversion-Explosive/IEDP COI is associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each Explosive/IEDP COI at the asset.
- If **no** Theft/Diversion Explosive/IEDP COI is associated with this asset, you will **not** see the Explosive/IEDP COI screen.

Question #	SVA Question	Question Details
[Q:3.51-8858]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Theft/Diversion-Explosive/IEDP COI. Select only one chemical as the Primary COI for this asset. Since only one chemical can be listed as the Primary COI, assets with multiple COIs that should be the Primary COI will need to be defined as multiple assets.
[Q:3.51-9167]	Is the facility's largest inventory of the COI at this asset?	You will need to answer this question for each Explosive COI at the asset. Answer Yes if the asset contains the largest inventory of the COI.
[Q:3.51-5534]	Is the COI shipped offsite from this asset?	You will need to answer this question for each Explosive COI at the asset. Answer Yes if the COI is shipped offsite from this asset.

If you indicated that the asset's primary security issue is a Theft/Diversion Explosive/IEDP COI, the following questions will be asked about the Primary COI:

Question #	SVA Question	Question Details
[Q:3.52-9171]	COI concentration range.	Use the drop-down list box provided to select the concentration range of the COI in this packaging type (% by weight).
[Q:3.52-9172]	Packaging type description.	Enter a brief description of the packaging type. Possible examples of transportation packaging include: • Bottles • Totes • Carboys • Boxes • Drums • Pressurized portable tanks and cylinders
[Q:3.52-9174]	Transportation packaging type.	Use the drop-down list box provided to select the transportation packaging type.
[Q:3.52-9173]	Total quantity of COI in this packaging type (lbs).	Enter the total quantity for this packaging type.

NOTE: For chemicals that have multiple concentrations and/or transportation packaging types at this asset, enter the first instance, complete the related questions, and then click the [Add] button. A new entry line will appear for additional instances. Continue adding entries until all applicable instances have been provided. Click the [Next] button when you are finished to continue.

6.2.2.5 *Theft/Diversion-Weapon of Mass Effect COI*

- If you indicate that a Theft/Diversion-WME COI is the primary security issue, you will be asked to identify the Primary COI and then provide detailed information about each chemical at the asset.
- If you indicate that a Theft/Diversion-WME COI is associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each WME COI at the asset.
- If **no** Theft/Diversion-WME COI is associated with the asset, you will **not** see the WME COI screen.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:3.49-8862]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Theft/Diversión- WME COI. Select only one chemical as the Primary COI for this asset. Because only one chemical can be listed as the Primary COI, assets with multiple COIs that should be the Primary COI will need to be defined as multiple assets.
[Q:3.49-9094]	Is the facility's largest inventory of the COI at this asset?	You will need to answer this question for each WME COI at the asset. Answer Yes if the asset contains the largest inventory of the COI.
[Q:3.49-5533]	Is the COI shipped offsite from this asset?	You will need to answer this question for each WME COI at the asset. Answer Yes if the COI is shipped offsite from this asset.

If you indicate that this asset's primary security issue is a Theft/Diversión WME COI, the following questions will be asked about the Primary COI:

Question #	SVA Question	Question Details
[Q:3.5-9096]	COI concentration range.	Use the drop-down list box provided to select the concentration range of the COI in this packaging type (% by weight).
[Q:3.5-9097]	Packaging type description.	Enter a brief description of the packaging type. Possible examples of transportation packaging include: • Bottles • Totes • Carboys • Boxes • Drums • Pressurized portable tanks and cylinders
[Q:3.5-9098]	Transportation packaging type.	Use the drop-down list box provided to select the transportation packaging type.

Question #	SVA Question	Question Details
[Q:3.5-9165]	Total quantity of COI in this transportation packaging type (lbs).	Enter the total quantity for this packaging type.

NOTE: For chemicals that have multiple concentrations and/or transportation packaging types at this asset, enter the first instance, complete the related questions, and then click the [Add] button. A new entry line will appear for additional instances. Continue adding entries until all applicable instances have been provided. Click the [Next] button when you are finished to continue.

6.2.2.6 *Theft/Diversion-Chemical Weapons/Chemical Weapons Precursor Chemical of Interest*

- If you indicate that a Theft/Diversion-CW/CWP was the primary security issue, you will be asked to identify the Primary COI and then provide detailed information about each chemical at the asset.
- If you indicate that a Theft/Diversion-CW/CWP is associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each CW/CWP at the asset.
- If **no** Theft/Diversion-CW/CWP is associated with the asset, you will **not** see the CW/CWP COI screen.

Question #	SVA Question	Question Details
[Q:3.47-8860]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Theft/Diversion-CW/CWP COI. Select only one chemical as the Primary COI for this asset. Because only one chemical can be listed as the Primary COI, assets with multiple COIs that should be the Primary COI will need to be defined as multiple assets.
[Q:3.47-9008]	Is the facility's largest inventory of the COI at this asset?	You will need to answer this question for each Theft/Diversion-CW/CWP COI at the asset. Answer Yes if the asset contains the largest inventory of the COI.
[Q:3.47-5532]	Is the COI shipped offsite from this asset?	You will need to answer this question for each Theft/Diversion-CW/CWP COI at the asset. Answer Yes if the COI is shipped offsite from this asset.

If you indicate that the asset's primary security issue is a Theft/Diversion-CW/CWP COI, the following questions will be asked about the Primary COI:

Question #	SVA Question	Question Details
[Q:3.48-9011]	COI concentration range.	Use the drop-down list box provided to select the concentration range of the COI in this packaging type (% by weight).
[Q:3.48-9031]	Packaging type description.	Enter a brief description of the packaging type. Possible examples of transportation packaging include: • Bottles • Totes • Carboys • Boxes • Drums • Pressurized portable tanks and cylinders
[Q:3.48-9032]	Transportation packaging type.	Use the drop-down list box provided to select the transportation packaging type.
[Q:3.48-9091]	Total quantity of COI in this transportation packaging type (lbs).	Enter the total quantity for this packaging type.

NOTE: For chemicals that have multiple concentrations and/or transportation packaging types at the asset, enter the first instance, complete the related questions, and then click the [Add] button. A new entry line will appear for additional instances. Continue adding entries until all applicable instances have been provided. Click the [Next] button when you are finished to continue.

6.2.2.7 Sabotage/Contamination Chemical of Interest

- If you indicate that a Sabotage/Contamination COI is the primary security issue, you will be asked to identify the Primary COI and then provide detailed information about each chemical at the asset.
- If you indicate that a Sabotage/Contamination COI is associated with the asset but it is **not** the primary security issue, you will be asked detailed information about each Sabotage/Contamination COI at the asset.
- If **no** Sabotage/Contamination COI is associated with this asset, you will **not** see the Sabotage/Contamination COI screen.

Question #	SVA Question	Question Details
[Q:3.53-8864]	Indicate the Primary COI for this asset.	You will need to answer this question if you indicated that the asset's primary security issue was a Sabotage/Contamination COI. Select only one chemical as the Primary COI for this asset. Since only one chemical can be listed as the Primary COI, assets with multiple COI that should be the Primary COI will need to be defined as multiple assets.
[Q:3.53-3632]	Quantity.	You will need to answer this question for each Sabotage/Contamination COI at the asset. Enter the quantity (in pounds) at this asset.
[Q:3.47-9008]	Is the facility's largest inventory of the COI at this asset?	You will need to answer this question for each Sabotage/Contamination COI at the asset. Answer Yes if the asset contains the largest inventory of the COI.

6.2.3 Cyber Control and Business Systems

Cyber control systems are defined as systems that have the ability to control the chemical process(es) and whose failure or misuse could result in a COI release, theft/diversion, or sabotage. (See Section 6.3 for more details.) Possible examples of these types of systems include:

- SCADA systems
- Distributed Control Systems (DCS)
- Process Control Systems (PCS)
- Industrial Control Systems (ICS).

Cyber business systems are defined as information systems that are intended to improve the competitive position of an organization or support the corporate strategy of an organization. (See Section 6.4 for more details.)

You will be asked the following questions about cyber control system(s) and cyber business system(s) at the asset:

Question #	SVA Question	Question Details
[Q:3.56-3659]	Is there a cyber control system related to this asset?	Provide a Yes or No answer to this question.
[Q:3.561-4292]	Is there a cyber business system related to this asset?	<i>You will need to answer this question if you indicated that the asset's primary security issue is Theft/Diversion.</i> Provide a Yes or No answer to this question.

6.2.4 Asset Completion

The last screen of the **Asset Characterization** section will ask you if all of the questions are completed for the asset.

- If all asset characterization information is complete, select the checkbox next to the asset and click the [Next] button to continue. When you indicate that the questions are complete, you will be returned to your inventory list of assets (see Picture 6.3).
- If you marked the asset as being complete and that all required questions were answered for that asset, the asset will feature a green **Complete** icon. If you do not check the box to indicate that the asset's questions are complete, or if any required questions were not answered, the asset will feature a yellow **Incomplete** icon. You can reference the green and yellow icons as reminders of the status of each asset.
- Repeat this process for each facility asset. When all asset descriptions have been completed, answer the question at the bottom of the asset inventory screen, "Have all assets been listed and described?" Select Yes and click the [Next] button to continue.

The screenshot shows a web application interface for 'Asset Name Inventory'. At the top, there is a header bar labeled 'Asset Name'. Below it, a small text label '[Q:3.1-3413]' is visible. The main area contains a list of three assets, each with a text input field, a 'Delete' button, and a 'Describe' button. To the right of each 'Describe' button is a green box containing a checkmark and the word 'Complete'. The assets listed are: 'Tank 123 - Acrolein - Release', 'Tank 456 - Propylene - Release', and 'R&D Lab - Arsenic Trichloride - Theft/Diversion'. At the bottom of the list, there is an empty text input field and an 'Add' button.

Picture 6.3: Asset Name Inventory with Complete Icons

6.3 Cyber Control Systems

If you indicated that the facility has at least one cyber control system and has at least one asset with a primary security issue that is **not** Theft/Diversion, you will be asked to identify the cyber control system by entering its name on the text box provided on the **Cyber Control System** screen and then click the [Add] button next to it (as seen in Picture 6.4). **NOTE:** The cyber control systems you enter should be limited to those that have the ability to control the chemical process and could result in a release or contamination. See Section 6.2.3 for more details.

The screenshot shows a web application interface for 'Cyber Control System Name'. At the top, there is a header bar labeled 'Control System Name'. Below it, a small text label '[Q:3.7-3711]' is visible. The main area contains a large text input field and an 'Add' button to its right.

Picture 6.4: Cyber Control System Name Text Box

After you add the first cyber control system, the following changes will happen to the screen:

- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that cyber control system from your submission.
- Another text box and [Add] button will appear the first that will allow you to add additional cyber control systems. You can submit as many cyber control systems as needed.
- A [Describe] button will appear to the right of the text box where you entered the cyber control system's name.

To submit a detailed description of the cyber control system, click the [Describe] button. A new screen will appear which will require you to provide details regarding the following questions:

Question #	SVA Question	Question Details
[Q:3.71-3719]	Enter cyber control system description	Enter a description of the cyber control system
[Q:3.71-3835]	Is the asset controlled with this control system?	The bottom section of the screen will show the assets identified earlier in the Asset Characterization section. Select Yes or No to identify the individual asset with the control system. A control system can be associated with multiple assets.

When you are finished describing the cyber control system, click the [Next] button on the bottom of the screen to continue. You will be returned to the first **Cyber Control System** screen. When all cyber control systems have been named and descriptions have been completed, answer the question at the bottom of the screen, "Have all relevant cyber control systems been identified?" Select Yes and click the [Next] button to continue.

NOTE: Facilities with assets that **only** have Theft/Diversion as their primary security issue will **not** see the **Cyber Control System** screen, even if the facility has responded that they have a cyber control system.

6.4 Cyber Business Systems

If you indicated that the facility has at least one cyber business system, you will be asked to identify the cyber business system by entering its name on the text box provided on the **Cyber Business System** screen and then clicking the [Add] button next to it.

Possible examples of these types of systems include business management systems such as SAP™ or inventory management systems. See Section 6.2.3 for more details.

After you add the first cyber business system, the following changes will happen to the screen:

- The [Add] button will change to a [Delete] button, which you can use if you choose to delete that cyber business system from your submission.
- Another text box and [Add] button will appear the first that will allow you to add additional cyber business systems. You can submit as many cyber business systems as needed.
- A [Describe] button will appear to the right of the text box where you entered the cyber business system's name.

To submit a detailed description of the cyber business system, click the [Describe] button. A new screen will appear which will require you to provide details regarding the following questions:

Question #	SVA Question	Question Details
[Q:3.81-3720]	Enter cyber business system description	Enter a description of the cyber business system
[Q:3.81-3837]	Is the asset associated with this business system?	The bottom section of the screen will show the assets identified earlier in the Asset Characterization section. Select <i>Yes</i> or <i>No</i> to associate the individual asset with the business system. A business system can be associated with multiple assets.

When you are finished describing the cyber business system, click the [Next] button on the bottom of the screen to continue. You will be returned to the first **Cyber Business System** screen. When all cyber business systems have been named and descriptions have been completed, answer the question at the bottom of the screen, "Have all relevant cyber business systems been evaluated?" Select *Yes* and click the [Next] button to continue.

7. Vulnerability Analysis

The **Vulnerability Analysis** section of the SVA process allows you to provide input based on an assessment of the facility's vulnerability to the specific attack scenarios selected by the SVA team. Consistent with CFATS requirements, this portion of the CSAT SVA must also ask questions related to the facility's Threat Assessment, Risk Assessment, and Countermeasures Analysis.

NOTE: The vulnerability factors documented as part of the CSAT SVA should be based on the expected performance of existing security measures, **not** measures the facility plans to implement in the future.

7.1 Facility Security Issues Analysis

The **Vulnerability Analysis** section begins with a summary screen that highlights assets and security issues. The information on this screen should be reviewed for accuracy.

Vulnerability Analysis

« Back

Next »

Facility Security Issues to Be Analyzed

Asset Name	Release Toxic	Release Flammable	Release Explosive	Theft/ Diversion EXP/IEDP	Theft/ Diversion WME	Theft/ Diversion CW/CWP	Sabotage/ Contamination
[Q:6.0-4932]	[Q:6.0-4933]	[Q:6.0-4934]	[Q:6.0-4935]	[Q:6.0-4938]	[Q:6.0-4937]	[Q:6.0-4936]	[Q:6.0-4939]
Tank 123 - Acrolein - Release	✓						
Tank 456 - Propylene - Release		✓					
R&D Lab - Arsenic Trichloride - Theft/Diversion						✓	

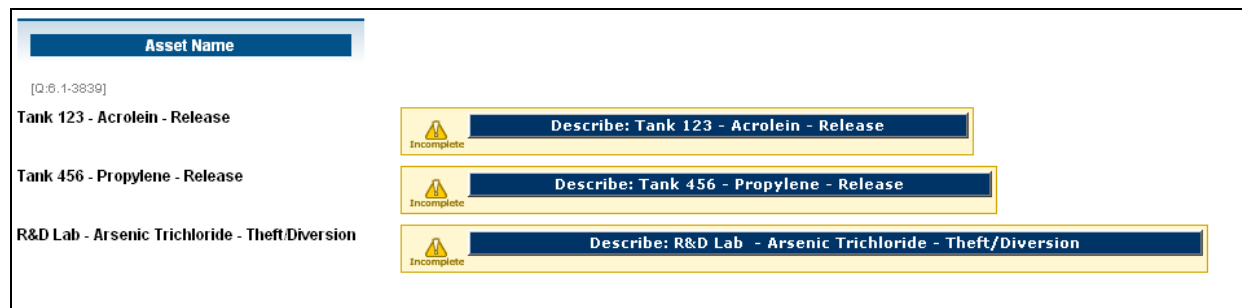
Picture 7.1: Asset and Security Issues Summary Screen

After you finish reviewing the summary screen, click the [Next] button on the bottom of the screen to begin a vulnerability analysis on each listed asset.

7.2 Introduction Screen

This **Vulnerability Analysis** section follows a process that is similar to the previous sections. You will be presented with the assets you submitted earlier, and for each you will need to:

- Locate the asset on the facility map; and
- Complete the attack modes relevant to the asset. For each attack mode, you will need to select the most relevant attack scenario and answer vulnerability questions.



The screenshot displays the 'Asset Vulnerability Analysis' screen. At the top, there is a header 'Asset Name'. Below it, a list of assets is shown, each with a status indicator and a 'Describe' button. The assets are:

- Tank 123 - Acrolein - Release (Status: Incomplete)
- Tank 456 - Propylene - Release (Status: Incomplete)
- R&D Lab - Arsenic Trichloride - Theft/Diversion (Status: Incomplete)

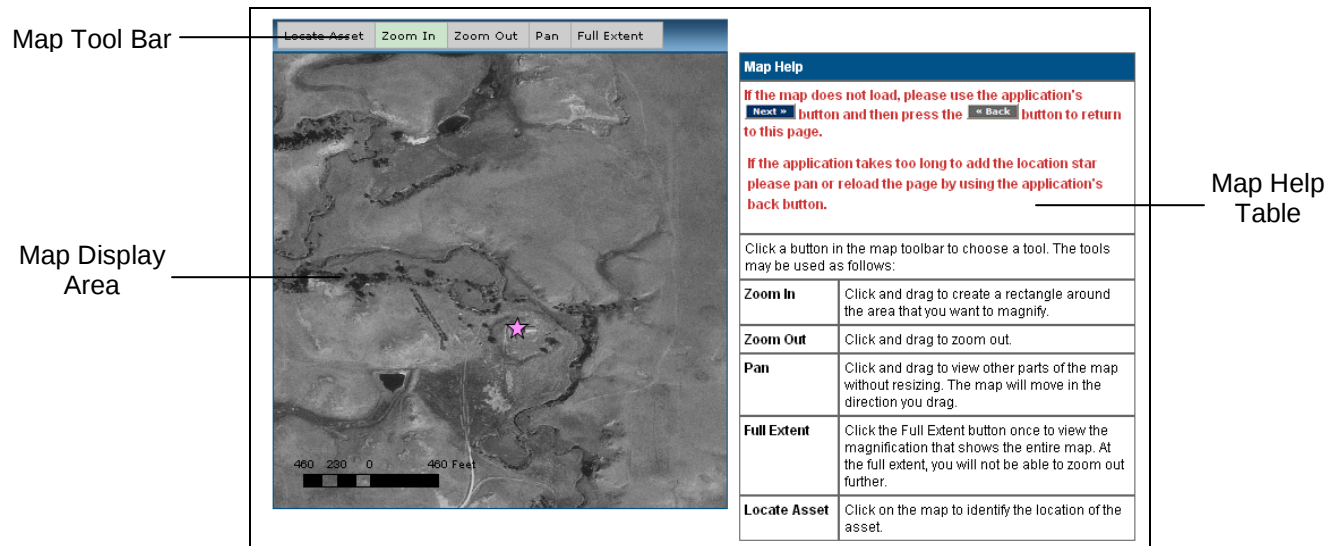
Each asset entry has a yellow box with a warning icon and the text 'Incomplete' next to it. To the right of each asset name is a blue button with the text 'Describe: [Asset Name]'.

Picture 7.2: Asset Vulnerability Analysis Screen

To begin the vulnerability analysis on an asset, click the [Describe] button on the **Asset Vulnerability Analysis** screen. This will direct you to the **Asset Location** screen.

7.3 Asset Location

The **Asset Location** screen allows you to identify the location of the asset on an interactive aerial map of the facility and its immediate surrounding area. There are two primary features to assist the user with map navigation: the map tool bar and the associated map help table, which provides information on how to use the map tool bar.



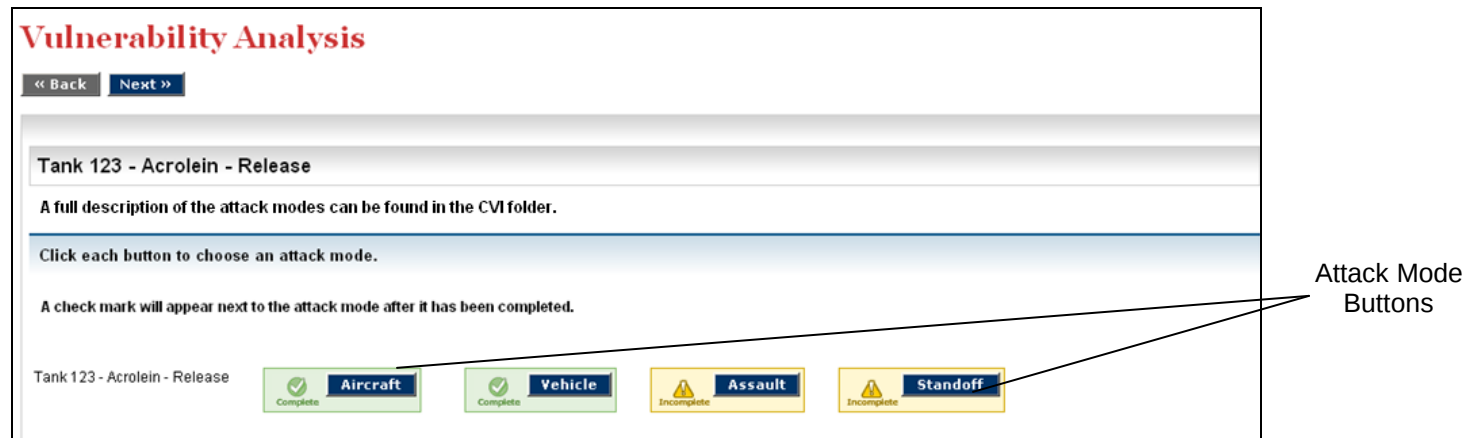
Picture 7.3: Asset Location Screen

- The map tool bar features the following functions:
 - **Panning:** Click the [Pan] button to navigate within the map to find the asset. After clicking [Pan], place your pointer within the map display area, hold down your left mouse button, and drag the map to the desired location. Click the [Pan] button again to deactivate the pan function.

- o **Zooming In:** Click the [Zoom In] button to increase the magnification of the map display area where the asset is located. After clicking the [Zoom In] button, place your pointer near the place within the map display area you would like to magnify. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be magnified. You can continue to use this method to zoom to the level of magnification that is sufficient for locating the asset. Click the [Zoom In] button again to deactivate the magnification function.
- o **Zooming Out:** Click the [Zoom Out] button if additional adjustment to the map display area is necessary to allow for a wider view. After clicking the [Zoom Out] button, place your pointer near the place within the map display area you would like to contract. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be contracted. Click the [Zoom Out] button again to deactivate the contraction function.
- o **Full Extent:** Click the [Full Extent] button to reset the map to its fullest view. Repeat the steps described above until the asset is clearly identified.
- o **Locate Asset:** Click the [Locate Asset] to pinpoint the location of the asset on the map. Clicking the [Locate Asset] button will allow you to use your pointer to place a visible identifier, a pink star , on the map at the asset location. Click the [Locate Asset] button again to deactivate the location function.
- Once you are satisfied that the asset has been located and that you have successfully placed an image of the asset within the map display area, click the [Next] button at the bottom of the screen. **NOTE:** Do **not** click the [Next] button until you place the pink star on the map.

7.4 Attack Modes

After you have successfully located the asset, you will see a series of **Attack Mode** screens. **NOTE:** For each asset, only the attack modes that pertain to that asset will appear. (For example, a facility that is not on a navigable waterway will **not** need to answer Maritime scenario questions.)



Picture 7.4: Attack Mode Selection Screen

To begin, click the first attack scenario button on the **Attack Mode Selection** screen and complete the questions. Up to seven attack modes are possible:

- Vehicle Borne Improvised Explosive Device (VBIED)
- Maritime
- Aircraft
- Theft
- Diversion

- Sabotage
- Assault Team
- Standoff

For each set of **Attack Mode** screens, you will use the map image you selected of the asset as reference to complete the following steps:

1. **Select an Attack Scenario:** You may select from one of the standard attack scenario descriptions, or describe a facility-specific scenario to reflect vulnerabilities or consequences that are specific to the facility's arrangement and security systems. Detailed descriptions of the attack scenarios are available online at csat.dhs.gov/csat.
2. **Identify Attack Location – Damage Circles:** The CSAT SVA identifies the attack location for all attacks against assets with a Release security issue as the Primary COI. Damage circles will display on the map to provide the facility with a visual reference for answering the vulnerability factors.
 - o For Maritime, Vehicle, and Standoff scenarios, an attack location will need to be identified by the facility.
 - o For Aircraft and Assault scenarios, the attack location is assumed to be the center of the asset.
 - o Theft and Sabotage scenarios do **not** display damage circles.

The following table shows the distances to the listed overpressure levels for each of the scenarios applicable to assets with Release security issues.

Attack Scenario	Radius of Outer Damage Circle (3 psi)	Radius of Inner Damage Circle (9 psi)
Aircraft	950 ft	490 ft
Maritime	270 ft	140 ft
Vehicle	340 ft	170 ft
Assault	110 ft	55 ft

NOTE: The Standoff scenario displays only one circle that represents a weapon range of 657 feet.

3. **Attack Scenario Questions:** For Maritime, Vehicle, and Standoff scenarios, you must determine if the asset is within the inner damage circle. When completing a Theft, Diversion, or Sabotage scenario, the user will **only** answer questions regarding the Primary COI at risk.
 - o If the asset is within the outer damage circle or you are completing an Aircraft or Assault Team scenario, you will need to determine the population within the inner damage circle.
 - o If the asset is **not** within the inner damage circle, your vulnerability analysis for the asset is complete at this point. (For example, a navigable waterway was identified but an attack from the waterway would not affect the asset, so the vulnerability analysis is complete.)
4. **Vulnerability Factors:** For each attack scenario, you will answer a series of vulnerability factor questions. These questions will vary, depending on the attack scenario.
5. **Release Questions:** For Release scenarios, you will answer specific Release questions.

When an attack mode analysis is completed, you will be returned to the **Attack Mode Selection** screen. The attack scenario button you selected will now display a green **Complete** status icon. You will then select another scenario on the **Attack Mode Selection** screen to continue the analysis.

7.4.1 Attack Scenario Selection

For each asset and attack mode, you will see an **Attack Scenario Selection** screen.

Aircraft Scenario

Select one standard scenario below OR choose "Other" to provide an alternative scenario description.

For each Attack Scenario the user may select from one of the standard attack scenario descriptions or identify a new scenario that better reflects a facility's situation. For each asset and attack mode, select a standard attack scenario that applies to the facility and to which the asset would be most vulnerable (compared to the other standard scenarios). If there is another attack scenario (i.e., not one of the standard scenarios) to which the asset would be more vulnerable, use the "other" option and evaluate it instead of one of the standard scenarios.

- ☐ A1 - Medium-range, medium-lift aircraft (i.e., 737 size) crashes into facility in attempt to destroy large storage tanks of COI located in the tank farm area, separate from other process equipment.
- ☐ A2 - Adversary crashes medium-range, medium-lift aircraft (i.e., 737 size) into facility in attempt to destroy large chemical processing area containing a variety of process equipment, including in-process inventories of COI.
- ☐ Other - User defined scenario.

Picture 7.5: Attack Scenario Selection Screen

On the **Attack Scenario Selection** screen, you can:

- Use the option buttons to select an attack scenario from one of the descriptions provided that applies to the facility and to which the asset would be most vulnerable (in comparison to the other standard scenarios); or
- Use the **Other – User defined scenario** option button to identify another attack scenario (i.e., not one of the standard scenarios) that better reflects a facility's situation and to which the asset would be more vulnerable.

If you selected **Other – User defined scenario**, you will be asked to describe the attack scenario relevant to the asset. The description should include information such as the assumed point of attack and its sequence of events.

Detailed descriptions of the attack scenarios may be found in the *CSAT SVA Attack Scenario Descriptions* document, which is available online at csat.dhs.gov/csatsat to active CSAT users who have completed CVI training and have started their SVAs. The table below provides brief descriptions of the standard attack scenarios for each attack mode.

Attack Mode	Standard Attack Scenario Descriptions
Aircraft Crash Attack	• A1: Commercial aircraft (i.e., 737 size) crashes into facility in attempt to destroy large storage tanks of COI located in the tank farm area, separate from other process equipment. • A2: Adversary crashes commercial aircraft (i.e., 737 size) into facility in attempt to destroy large chemical processing area containing a variety of process equipment, including in-process inventories of COI.
VBIED	• V1: Adversary places VBIED outside of the facility perimeter, but located close enough (i.e., within 340 feet) for the vehicle bomb to destroy the COI storage tank or area considered the asset. • V2: The adversary cuts the facility back gate open during off hours (i.e., night or weekend operation) and drives the VBIED to a location at the end of the secondary containment closest to tank/area that is this asset. • V3: The adversary accesses the facility with a VBIED by entering the plant site behind a vehicle making an authorized entry or by crashing through a controlled access gate. The adversary drives the VBIED to the storage area or process unit that represents this asset and detonates the device there.
Maritime/Boat Borne IED Attack	• B1: Adversary drives boat carrying IED on an offsite waterway that comes within 370 feet of the asset and explodes the boat at the closest approach point to the asset. • B2: Adversary drives boat carrying IED into an onsite waterway or channel that comes within 370 feet of the asset and explodes the boat at the closest approach point to the asset.

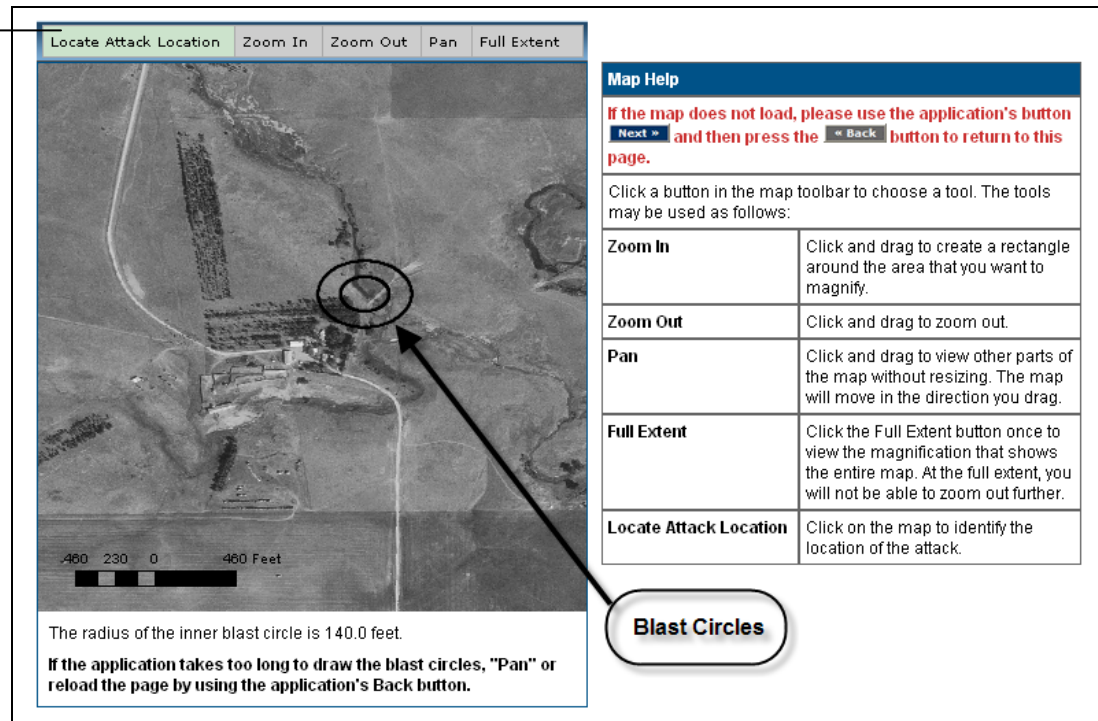
CSAT Security Vulnerability Assessment Application Instructions

Attack Mode	Standard Attack Scenario Descriptions
Assault Team Attack	• AT1: Adversary team climbs or cuts the facility perimeter fence and places two explosive charges against the asset. • AT2: Adversary assault team attacks security assets at access control point and then moves through the plant on foot and places two explosive charges on this asset.
Standoff Attack	• SO1: Adversary accesses the facility and fires the stand-off weapon (i.e., light anti-tank weapon with shaped charge warhead) into the asset from a distance of 100 meters, initiating a release of a COI. • SO2: The facility is surrounded by a contiguous 7 ft. in height chain-link fence. Asset is within 100 meters of the facility perimeter and is easily visible from outside the fence. The adversary drives a van or delivery truck into the parking lot of an adjacent facility and uses the top of the vehicle as an elevated platform to launch a stand-off weapon (i.e., light anti-tank weapon with shaped charge warhead) at the asset from a distance of 100 to 200 meters.
Theft	• T1: Adversary team enters the facility and steals largest portable container on site, leaving the facility in a vehicle without immediate awareness by facility staff (i.e., no immediate law enforcement notification and pursuit). • T2: Adversary team enters the facility in a vehicle, obtains one or more portable containers of the theft COI, and successfully leaves the facility in the vehicle without being detected. • T3: Adversary enters the facility on foot and steals one or more man-portable containers, moving them to transport vehicles outside of the facility.
Sabotage	• SA1: Adversary (insider or outsider) accesses placarded amount of COI that is designated for shipment and contaminates largest placarded amount/shipment from the facility in a manner that will result in an explosion or toxic release at some point after shipped from the facility. • SA2: Adversary (insider or outsider) accesses placarded amount of COI designated for shipment and contaminates one or more placarded amounts (selecting shipments that are easily contaminated). The containers are then shipped from the facility and the contamination results in an explosion or toxic release at some point after shipped from the facility.
Diversion	• D1: Adversary is allowed to register as a customer to purchase COI and have it shipped to the adversary's chosen location. • D2: Adversary is allowed to file a false order for an existing customer that results in shipping the COI to a location that is not controlled by the approved customer. • D3: Adversary is allowed to accept shipment of or pick up an order with COI that is intended for an approved customer.

7.4.2 Attack Location Map

After selecting an attack scenario, you will need to identify an attack location for Maritime, Vehicle, and Standoff attack scenarios. You will do this on the **Location of Attack** screen, which features navigational functionality which is similar to the **Asset Location** screen described in Section 7.3. The map tool bar on the **Location of Attack** screen includes a [Locate Attack Location] button in place of the [Locate Asset] button, as seen in Picture 7.6.

Locate Attack
Location Button



Picture 7.6: Location of Attack Screen

- Click the [Locate Attack Location] button after the aerial photo appears on the **Location of Attack** screen. Use your pointer to select on the map the area near the asset location to identify the attack location that will achieve the maximum damage.
NOTE: For a Maritime attack, the location will need to be on a navigable waterway (i.e., not on land) even if the asset is not located within the blast. When selecting an attack location, be sure to include the asset and other collateral sub-targets to generate the greatest potential consequence. For example:
 - If the Primary COI of the asset being attacked is a Release-Toxic COI, identify the location of the attack that results in the greatest amount of the specific Release-Toxic COI released.
 - If the Primary COI of the asset being attacked is a Release-Flammable COI, identify the location of the attack that results in the greatest amount of Release-Flammable COI released.
 - If the Primary COI of the asset being attacked is a Release-Explosive COI, identify the location of the attack that results in the greatest amount of Release-Explosive COI released.
- After you make your selection, wait for the damage circles to appear. Use the [Zoom] button to magnify the map area around the blast circles. This image will appear on the next screen for reference, but printing this page is also recommended. Click the [Next] button to proceed with the vulnerability analysis. **NOTE:** Do **not** click the [Next] button at the bottom of the screen until the blast circles appear on the map.

7.4.3 Attack Scenario Questions

For Maritime, Vehicle, and Standoff Attack Scenarios: You must determine if the asset is within the inner damage circle you created on the **Location of Attack** screen. Use the map with the damage circles to answer the following questions:

Question #	SVA Question	Question Details
[Q:7.2-1531]	Maritime: Is any portion of the asset within the inner damage radius (140 feet)?	- In most cases, you would answer Yes to these questions. If the asset is located within the inner damage circle, you will be directed to further attack screens. - There may be situations when physical constraints place the asset outside of the inner damage circle (e.g., no waterway near the asset). In these cases, you would select the <i>No</i> option button. If no assets are located in the inner damage circle, you will be directed to conclude the attack consequence analysis.
[Q:8.2-9626]	Vehicle: Is any portion of the asset within the inner damage radius (170 feet)?	
[Q:11.2-10337]	Standoff: Is any portion of the asset within the range of the standoff weapon (657 feet)?	

For all Aircraft and Assault Attack Scenarios, and Qualifying Maritime and Vehicle Attack Scenarios:

Question #	SVA Question	Question Details
[Q:9.21-4063]	Aircraft: What is the expected number of people at the facility within the outer damage radius (950 feet)?	The numbers you submit for these population questions should represent the typical maximum number of full-time employees and resident contractors within the combined inner and outer areas at any given time. Do not include occasional times when there is a higher on-site workforce in this number, such as during turnarounds.
[Q:10.21-4080]	Assault: What is the expected number of people at the facility within the outer damage radius (110 feet)?	
[Q:7.21-3896]	Maritime: What is the expected number of people at the facility within the outer damage radius (270 feet)?	
[Q:8.21-3995]	Vehicle: What is the expected number of people at the facility within the outer damage radius (340 feet)?	

For Diversion Attack Scenarios:

Question #	SVA Question	Question Details
[Q:12.6-7736]	Is the customer permitted to pick up orders at this asset?	The answer you provide to this question will determine which vulnerability factor questions are asked later.

For Theft, Diversion, and Sabotage Attack Scenarios:

Question #	SVA Question	Question Details
[Q:12.2-11343, Q:13.2-11372]	Quantity of COI at Risk in this scenario (pounds)	Answer questions regarding the material at risk. The COI is listed on the screen.
[Q:12.2-11344, Q:13.2-11373]	Percent Concentration by Weight in this scenario.	

7.4.4 Vulnerability Factor Questions

The vulnerability factor questions allow you to select the vulnerability factor value which best represents the vulnerability situation for the attack mode for a specific asset. After you select the vulnerability factor value, you have the opportunity to document any assumptions you made in assigning that value. The **Assumption** text box is optional; however, providing some assumption information will help DHS understand the facility's rationale for the vulnerability factor assignment. **NOTE:** The vulnerability analysis for assets with Theft/Diversion and Sabotage scenarios does **not** involve answering vulnerability factor questions.

The vulnerability factor questions cover the following areas:

- **Identifiability Probability:** This refers to the probability that the adversary can identify the specific target asset during the course of planning and executing an attack. Identifiability is a function of the size, labeling, and nature of the asset and its similarity to others at the facility. When estimating identifiability, you should consider it difficult for an adversary to distinguish between several similar items of equipment, only some of which would be viable targets. The labeling of equipment is also a factor in this assessment.
- **Accessibility Probability:** This refers to the probability that an adversary is successful in reaching the location that they must access to successfully execute an attack, given the security measures currently implemented at the facility. The accessibility factor should reflect the ability of existing security systems and processes to prevent the adversary from reaching a location close enough to the asset to launch the specific type of attack (i.e., close enough to place an explosive device or use a standoff weapon). **NOTE:** The security measures considered for this probability should **not** include facility or offsite security force response capability and actions.
- **Facility Security Response Force Capability:** This refers to the probability that a facility (i.e., onsite) security response force, if any, is able to interdict an adversary force before it succeeds in executing an attack (assuming that the security measures alone were not adequate). This vulnerability factor reflects the ability of the onsite security force to intervene in time to stop a specific type of attack. Assume that the accessibility controls considered in determining accessibility probably would **not** have stopped the adversary, but would have offered a delay consistent with the types of physical security measures at the facility.
- **Offsite Security Response Force Capability:** This refers to the probability that an offsite security response force, if any, is able to interdict an adversary force before it is successful in executing an attack (assuming that the onsite force failed). The likelihood of success of an offsite response force may be low, unless the facility has coordinated with local law enforcement and integrated them into facility planning, including exercises. Likewise, the staffing, training, and equipment of the response force for the type of attack should be considered before credit is given for response force effectiveness in interdicting an attack.

- **Achievability Probability:** This refers to the probability that an adversary could execute a successful attack (assuming the absence of all security measures). Achievability is a function of the inherent difficulty for the adversary to attack the specific target asset. Factors which may contribute to an achievability probability of less than 1.0 could include:
 - o Inaccuracy of a standoff weapon
 - o Difficulty in attacking a point target with the specified aircraft, particularly if the asset is among many other pieces of equipment or units
 - o Difficulty in loading a large but portable package
 - o Difficulty in effectively contaminating a COI shipment.
- **Target Hardness Probability:** This refers to the probability that an adversary who reached a target and executed the attack did not damage the asset sufficiently to cause the intended COI release event onsite or successfully steal/divert the COI for use in an attack. This factor represents the inherent hardness or location of the target that protects it from the effects of an attack that was successfully initiated. **NOTE:** Do **not** give additional credit for considerations you have already credited in evaluation of earlier factors (e.g., achievability, identifiability). Examples of situations where credit could be assessed include:
 - o Tanks located in a manner (e.g., underground or mounded) where an explosive device located at the closest point available would not necessarily cause its catastrophic failure.
 - o A vessel with multiple layers or insulation that provides spacing such that a standoff weapon would not be effective in penetrating the vessel.
 - o Hardware approaches that make theft of portable containers very difficult even when access is achieved.
 - o Other hardness situations the facility describes and justifies.Otherwise, the facility should assume the target asset is extremely unlikely to survive this kind of attack.
- **Availability Probability:** Use this factor to account for situations where the asset (or group of assets) only contains the applicable COI for a limited amount of time on a schedule that is not readily available to the adversary. For example, if the asset is a batch process tank that only contains the COI for one hour every 24 hours on a schedule that is not available or visible to the adversary, it can be determined that an attack is extremely **unlikely** to occur at a time when the asset contains a significant quantity of the COI. The Primary COI is listed here, as it is the applicable COI referred to in the availability probability questions.

- **Unauthorized Customer Registration (Diversion Scenarios Only):** This refers to the probability that an adversary can register himself/herself as a customer for purchase of the COI. This vulnerability assesses the probability of success or failure of the facility's customer validation procedures. For example, many customer validation programs verify:
 - (1) A customer's end use for the COI;
 - (2) The integrity of the customer's business operations;
 - (3) The customer's ability to pay and method of payment; and/or
 - (4) The customer's packaging and shipping requirements.

Another aspect of this vulnerability is the strength (or weakness) of the facility's cyber business system that maintains the approved customer list such that it prevents (or allows) the adversary to establish himself/herself as an approved customer.

- **Unauthorized Order Placement (Diversion Scenarios Only):** This vulnerability factor assumes the adversary who is not an authorized customer is misusing an established customer's account and can place an order for shipment to his/her chosen location. This factor is designed to assess an individual adversary's ability to defeat the facility's (or company's) procedures for identifying, validating, and vetting a customer seeking to purchase and receive delivery of a COI. For example, certain COI are prohibited from pick up and are always delivered directly to a customer by the facility. Other companies only ship to pre-determined and approved locations. This factor aims to assess the reliability of the facility's (or company's) order processing procedures.
- **Unauthorized Order Pick Up (Diversion Scenarios Only):** This refers to the probability that an adversary could pick up an order being held for an authorized customer. This vulnerability assumes that the adversary has **not** been able to place an order. Another possible factor in this assessment is the trustworthiness of the facility personnel involved in the physical packing, staging, and shipping processes. For example, the ability of the adversary to pick up an authorized customer's order could result from a facility's failure to secure its shipping and receiving.

All questions are listed in the following table, but only the ones that are applicable to the asset(s) will appear on screen. The wording of vulnerability factor questions may differ slightly, depending on the attack scenario.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:7.22-7276, Q:9.22-9687, Q:8.22-9609, Q:10.22-9767, Q:11.22-9900, Q:12.22-7657, Q:13.22-9948]	How likely is the adversary, in the course of planning and/or executing this attack scenario against this asset, to identify the specific asset(s) that must be attacked or stolen to achieve significant consequences?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each question. • Adversary is extremely unlikely to successfully identify the specific asset they desire to attack during this scenario. Prob(0 to 0.2) • Adversary is unlikely to successfully identify the specific asset they desire to attack during this scenario. Prob(0.2 to 0.4) • Adversary is equally likely to succeed or fail in identifying the specific target in the scenario. Prob(0.4 to 0.6) • Adversary success in identifying the specific target in the scenario is likely. Prob(0.6 to 0.8) • Adversary is almost certain to successfully identify the specific asset they desire to attack during this scenario. Prob(0.8 to 1.0) Document any important assumptions made in assessing identifiability.
[Q:7.22-7371, Q:8.22-9611, Q:10.22-9769, Q:11.22-9902, Q:12.22-7659, Q:13.22-9950]	How likely do you think it is that the adversary would be successful in breaching existing security measures and accessing a location from which they can attack the asset?	Check the box next to the answer that best describes the user's expectation for the scenario. Corresponding probabilities are shown next to each question. • Adversary is extremely unlikely to successfully access the asset. Prob(0 to 0.2) • Adversary is unlikely to successfully access the asset. Prob(0.2 to 0.4) • Adversary is equally likely to succeed or fail in accessing this asset with this attack. Prob(0.4 to 0.6) • Adversary is likely to successfully access the asset. Prob(0.6 to 0.8) • Adversary is almost certain to successfully access the asset. Prob(0.8 to 1.0) Document any important assumptions the SVA team made in assessing accessibility.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:7.22-7391, Q:8.22-9613, Q:10.22-9771, Q:12.22-7661, Q:13.22-9952]	How likely is the facility security response force to successfully interdict the adversary before they are successful in executing their attack (assuming that other security measures alone are not successful in stopping the attack)?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each question. • Facility security response force is almost certain to successfully interdict this type of attack. Prob(0.8 to 1.0) • Facility security response force is likely to successfully interdict this type of attack. Prob(0.6 to 0.8) • Facility security response force is almost equally likely to succeed or fail in interdicting this type of attack. Prob(0.4 to 0.6) • Facility security response force is unlikely to successfully interdict this type of attack. Prob(0.2 to 0.4) • Facility security response force is extremely unlikely to successfully interdict this type of attack. Prob(0 to 0.2) Document any important assumptions made in assessing facility security response force capability.
[Q:7.22-7412, Q:8.22-9615, Q:10.22-9773, Q:12.22-7663, Q:13.22-9954]	How likely is the designated offsite security response force (such as local law enforcement personnel) to successfully interdict the adversary before they are successful in executing their attack (given that the onsite team failed)?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each question. • Offsite security response force is almost certain to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0.8 to 1.0) • Offsite security response force is likely to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0.6 to 0.8) • Offsite security response force is almost equally likely to succeed or fail in interdicting this type of attack, assuming that the facility force was not successful. Prob(0.4 to 0.6) • Offsite security response force is unlikely to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0.2 to 0.4) • Offsite security response force is extremely unlikely to successfully interdict this type of attack, assuming that the facility force was not successful. Prob(0 to 0.2) Document any important assumptions made in assessing offsite security response force capability.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:7.22-7414, Q:9.22-9689, Q:8.22-9617, Q:10.22-9775, Q:11.22-9904, Q:12.22-7665, Q:13.22-9956]	How likely is the adversary to succeed in accomplishing this attack (giving no credit for any facility or asset security measures)?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each question. • Adversary is extremely unlikely achieve success with this attack even if security measures are not implemented. Prob(0 to 0.2) • Adversary is unlikely to achieve success with this attack even if security measures are not implemented. Prob(0.2 to 0.4) • Adversary is equally likely to succeed or fail in this attack if security measures are not implemented. Prob(0.4 to 0.6) • Adversary is likely to achieve success with this attack assuming security measures are not implemented. Prob(0.6 to 0.8) • Adversary is almost certain to achieve success with this attack assuming security measures are not implemented. Prob(0.8 to 1.0) Document any important assumptions made in assessing achievability.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:7.22-7416, Q:8.22-9619, Q:10.22-9777, Q:11.22-9906, Q:13.22-9958]	What is the probability that the asset would withstand the attack (i.e., suffers less than a catastrophic release/explosion or loss of COI to theft/diversion), assuming that the adversary is successful at accessing the target and executing the specific type of attack?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each answer. • The target is very hard against/resistant to this kind of attack, it is almost certain that this type of attack will not create a catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0.8 to 1.0) • The target is relatively hardened against/resistant to this type of attack, it is likely that this type of attack will not create a catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0.6 to 0.8) • The target is equally likely to withstand this type of attack or to fail (resulting in a catastrophic release, explosion, or loss of COI to theft/diversion). Prob(0.4 to 0.6) • The target is not very resistant to this type of attack and is unlikely to survive this type of attack without catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0.2 to 0.4) • The target is not resistant to this type of attack, and is extremely unlikely to survive this type of attack without catastrophic release, explosion, or loss of COI to theft/diversion. Prob(0 to 0.2) Document any important assumptions made in assessing target hardness.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:9.22-9694, Q:7.22-8911, Q:8.22-9624, Q:10.22-9782, Q:11.22-9911, Q:12.22-9361, Q:13.22-9961]	How likely is the specific asset attacked to contain the relevant COI, assuming that the adversary identifies and attacks the correct target asset?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each answer. • Attack is extremely unlikely to occur at a time the asset contains a significant quantity of the COI. Prob(0 to 0.2) • Attack is unlikely to occur at a time the asset contains a significant quantity of the COI. Prob(0.2 to 0.4) • Attack is equally likely to occur at a time the asset contains or does not contain a significant quantity of the COI. Prob(0.4 to 0.6) • Attack is likely to occur at a time the asset contains a significant quantity of the COI. Prob(0.6 to 0.8) • Attack is almost certain to occur at a time the asset contains a significant quantity of the COI. Prob(0.8 to 1.0) Document any important assumptions made in assessing availability.
[Q:12.8-7682]	How likely is the adversary to be able to register as a new customer that is approved to purchase theft/diversion COI?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each answer. • Adversary is extremely unlikely to successfully register as a new client to purchase the specific COI involved in this scenario. Prob(0 to 0.2) • Adversary is unlikely to successfully register as a new client to purchase the COI involved in this scenario. Prob(0.2 to 0.4) • Adversary is equally likely to succeed or fail in registering as a new client approved to purchase COI involved in this scenario. Prob(0.4 to 0.6) • Adversary is likely to succeed in registering as a new client approved to purchase COI. Prob(0.6 to 0.8) • Adversary is almost certain to successfully register as a new client authorized to purchase COI. Prob(0.8 to 1.0) Document any important assumptions made in assessing unauthorized customer registration.

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question	Question Details
[Q:12.8-7684]	How likely is the adversary to be able to place an order for this COI for an authorized customer that would allow shipment to a location where the adversary could accept the shipment?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each answer. • Adversary is extremely unlikely to successfully place an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0 to 0.2) • Adversary is unlikely to successfully place an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.2 to 0.4) • Adversary is equally likely to succeed or fail in placing an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.4 to 0.6) • Adversary is likely to succeed in placing an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.6 to 0.8) • Adversary is almost certain to successfully place an order for an existing client that would result in the specific COI being delivered to a location where the adversary could accept the shipment. Prob(0.8 to 1.0) Document any important assumptions made in assessing unauthorized order placement.

Question #	SVA Question	Question Details
[Q:12.8-7686]	How likely is the adversary to be able to pick up an order for an authorized customer for this COI?	Check the box next to the answer that best describes your expectation for the scenario. Corresponding probabilities are shown next to each answer. • Adversary is extremely unlikely to successfully pick up an order that is intended for pickup by an authorized customer. Prob(0 to 0.2) • Adversary is unlikely to successfully pick up an order that is intended for pickup by an authorized customer. Prob(0.2 to 0.4) • Adversary is equally likely to succeed or fail in picking up an order that is intended for pickup by an authorized customer. Prob(0.4 to 0.6) • Adversary is likely to succeed in picking up an order that is intended for pickup by an authorized customer. Prob(0.6 to 0.8) • Adversary is almost certain to successfully pick up an order that is intended for pickup by an authorized customer. Prob(0.8 to 1.0) Document any important assumptions made in assessing unauthorized order pick up.

7.4.5 Release Questions

The release scenario questions cover the following areas for Release COI:

- **COI Quantity (Pounds):** You will need to provide amount of COI the within the inner damage radius: Calculate the quantity by using the same counting rules provided by CFATS for calculating the STQs for the applicable Release COI.
- **Mitigation Factors:** If the Primary COI is a Release-Toxic COI and if any mitigation factors were identified in the **Asset Characterization** section, you will be asked if the mitigation factor(s) would survive the attack. If no mitigation factors were included, no questions will be displayed.

CSAT Security Vulnerability Assessment Application Instructions

The information below is for all release scenario questions, but only applicable questions will appear on the screen. Release scenario questions will vary, depending on the attack type.

Question #	SVA Question	Question Details
[Q:7.3-9170, Q:8.3-9636, Q:9.3-9706, Q:10.3-9793]	Release-Toxic COI: Quantity (pounds) within the inner damage radius	If the Primary COI is a Release-Toxic COI, enter total quantity of the same COI within the inner damage radius. The quantity entered here is calculated using the same counting rules that a facility applies in determining whether it meets or exceeds the STQ for this Release-Toxic COI.
[Q:7.4-9226, Q:8.4-9668, Q:9.4-9738, Q:10.4-9825]	Release-Flammable COI: Quantity (pounds) within the inner damage radius	If the Primary COI is a Release-Flammable COI, the total quantity should be for all flammable COI within the inner damage radius. The quantity entered here is calculated using the same counting rules that a facility applies in determining whether it meets or exceeds the STQ for this Release-Flammable COI.
[Q:7.5-9228, Q:8.4-9673, Q:9.5-9743, Q:10.5-9830]	Release-Explosive COI: Quantity (pounds) within the inner damage radius	If the Primary COI is a Release-Explosive COI, the total quantity should be for all explosive COI within the inner damage radius. The quantity entered here is calculated using the same counting rules that a facility applies in determining whether it meets or exceeds the STQ for this Release-Explosive COI.
[Q:7.3-9177, Q:8.3-9637, Q:9.3-9707, Q:10.3-9794, Q:11.3-9974]	Does the dike or berm containment survive the attack?	Provide a Yes or No answer for this question.
[Q:7.3-9191, Q:8.3-9638, Q:9.3-9708, Q:10.3-9795, Q:11.3-9975]	Does the leak detection system survive the attack?	Provide a Yes or No answer for this question.
[Q:7.3-9192, Q:8.3-9639, Q:9.3-9709, Q:10.3-9796, Q:11.3-9976]	Does the fixed vapor suppression system survive the attack?	Provide a Yes or No answer for this question.
[Q:7.3-9193, Q:8.3-9640, Q:9.3-9710, Q:10.3-9797, Q:11.3-9977]	Does the offsite notification system survive the attack?	Provide a Yes or No answer for this question.
[Q:7.3-9194, Q:8.3-9641, Q:9.3-9711, Q:10.3-9798, Q:11.3-9978]	Does the other mitigation measure survive the attack?	Provide a Yes or No answer for this question.

7.4.6 Completion of Vulnerability Analysis

When you finish the vulnerability analysis for an attack mode, click the [Next] button. You will be asked to confirm vulnerability analysis completion, and will then be returned to the **Attack Mode Selection** screen to select another attack mode for analysis.

NOTE: If you do *not* select the checkbox to confirm that the vulnerability analysis for an attack mode is complete, that attack mode will be displayed on the **Attack Mode Selection** screen with a yellow **Incomplete** icon. When you are finished completing vulnerability assets for all of the attack modes listed on the **Attack Mode Selection** screen, answer the question at the bottom of the screen, “Have vulnerability assessments been completed for all attack scenarios for all assets?” Select Yes and click the [Next] button to continue.

8. Computer Systems Analysis

The **Computer Systems Analysis** section of the SVA process allows you to provide input regarding the facility's computer systems. This section begins with the following questions:

Question #	SVA Question	Question Details
[Q:14.09-4151]	Are personnel allowed to carry portable cyber equipment into the facility (e.g., laptop computers, personal digital assistants (PDAs), flash drives, data disks, smart cell phones, etc.)?	Provide a Yes or No answer for this question.
[Q:14.09-4152]	Are personnel screened at facility entrances for unauthorized cyber related equipment?	Provide a Yes or No answer for this question.
[Q:14.091-4153]	Has the personnel screening process been validated through testing by professional security services?	Provide a Yes or No answer for this question.

8.1 Cyber Control Systems

If you identified any cyber control system earlier in the SVA, the **Cyber Control System** screen will be shown. You will need to answer the series of questions by selecting **Describe <Cyber Control System Name>** for each computer control system listed.

8.1.1 Mapping Cyber Control Systems

The **Cyber Control Location** screen allows you to identify the location of the asset's cyber control system on an interactive aerial map of the facility and its immediate surrounding area. There are two primary features to assist the user with map navigation: the map tool bar and the associated map help table, which provides information on how to use the map tool bar.

- The map tool bar features the following functions:
 - o **Panning:** Click the [Pan] button to navigate within the map to find the cyber control system. After clicking [Pan], place your pointer within the map display area, hold down your left mouse button, and drag the map to the desired location. Click the [Pan] button again to deactivate the pan function.
 - o **Zooming In:** Click the [Zoom In] button to increase the magnification of the map display area where the cyber control system is located. After clicking the [Zoom In] button, place your pointer near the place within the map display area you would like to magnify. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be magnified. You can continue to use this method to zoom to the level of magnification that is sufficient for locating the cyber control system. Click the [Zoom In] button again to deactivate the magnification function.
 - o **Zooming Out:** Click the [Zoom Out] button if additional adjustment to the map display area is necessary to allow for a wider view. After clicking the [Zoom Out] button, place your pointer near the place within the map display area you would like to contract. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be contracted. Click the [Zoom Out] button again to deactivate the contraction function.
 - o **Full Extent:** Click the [Full Extent] button to reset the map to its fullest view. Repeat the steps described above until the cyber control system is clearly identified.
 - o **Locate System:** Click the [Locate System] to pinpoint the location of the cyber control system on the map. Clicking the [Locate System] button will allow you to use your pointer to place a visible identifier, a pink star , on the map at the cyber control system location. Click the [Locate System] button again to deactivate the location function.
- Once you are satisfied that the cyber control system has been located and that you have successfully placed an image of the cyber control system within the map display area, click the [Next] button at the bottom of the screen. **NOTE:** Do *not* click the [Next] button until you place the pink star on the map.

8.1.2 Cyber Control System Questions

The following table lists the questions that you will need to answer about the asset's cyber control system. Provide a Yes or No answer for each question.

Question #	SVA Question
[Q:14.3-1614]	Is external access (e.g., Internet, modem, wireless) to cyber systems allowed?
[Q:14.31-1633]	Has the lack of external access been validated through testing by IT security professional services?
[Q:14.32-1635]	Are the capabilities of the cyber systems in the facility limited in regard to communications with portable cyber equipment (authorized or not) (e.g., laptop computers, personal digital assistants (PDAs), flash drives, data disks, smart cell phones)?
[Q:14.33-1637]	Has the disabling of communication capabilities been validated through testing by a professional IT security service?
[Q:14.34-1692]	Security Policy: Does the facility have documented and distributed cyber security policies, plans, and supporting procedures commensurate with the current information technology operating environment?
[Q:14.34-1693]	Security Policy: Does the facility have a documented and distributed cyber change management policy and supporting procedures (e.g., new hardware/software, employee access)?
[Q:14.34-1694]	Security Policy: Has an individual(s) been designated as responsible for cyber security at the facility?
[Q:14.34-2851]	Access Control: Does the facility allow systems to have external connections with portable electronic devices configured for minimum business needs and verified with scans?
[Q:14.34-1695]	Access Control: Does the facility practice the concept of least privilege (e.g., users are only granted access to those files and applications based on roles and responsibilities)?
[Q:14.34-1696]	Access Control: Have all default passwords been changed to user-specific passwords?
[Q:14.34-1697]	Access Control: Are accounts locked out after several unsuccessful login attempts?
[Q:14.35-1719]	Personnel Security: Does the facility perform background checks for personnel in critical/sensitive positions?
[Q:14.35-1720]	Personnel Security: Does the facility actively maintain the access control list to ensure that all cyber system accounts are modified, deleted, or de-activated as personnel leave the company or transfer into new roles?

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question
[Q:14.35-1721]	Physical and Environmental: Does the facility restrict physical access to sensitive or restricted IT, telecommunications, media storage, and control areas to those with appropriate need?
[Q:14.35-1723]	Awareness and Training: Does the facility provide cyber security training?
[Q:14.36-1727]	Monitoring and Incident Response: Does the facility log cyber security events on systems and review them on a regular basis?
[Q:14.36-2852]	Monitoring and Incident Response: Does the facility log cyber security events on servers, and review them on a regular basis?
[Q:14.36-1728]	Monitoring and Incident Response: Does the facility report significant cyber security events to senior management?
[Q:14.36-1730]	Monitoring and Incident Response: Does the facility mandate malicious code protection on all systems?
[Q:14.37-1735]	Monitoring and Incident Response: Does the cyber system allow email?
[Q:14.38-1737]	Monitoring and Incident Response: Are email attachments (e.g., executable files) filtered on incoming email?
[Q:14.39-1175]	Monitoring and Incident Response: Are there Safety Instrumented Systems (SIS) or other watch-dog systems, independent of the systems they monitor, that provide interlocks or response to prevent or mitigate catastrophic events and/or the consequences of a cyber attack?
[Q:14.4-1741]	Configuration Management: Has a business requirement been established for every external connection into the network/environment, including wireless and modem connections?
[Q:14.4-1742]	Configuration Management: Does the facility apply/perform regular software and hardware, patches, updates, upgrades, and replacements?
[Q:14.4-1743]	Configuration Management: Are configuration changes to the network and application's hardware and software reviewed by an IT security professional and by management to assess the security impact prior to the changes being implemented to the operational environment?
[Q:14.4-2854]	Risk and Vulnerability Management: Have potential vulnerabilities of critical assets, systems, and networks been identified and evaluated?
[Q:14.4-1744]	Risk and Vulnerability Management: Does the facility have a means to identify and measure cyber security risk (including requirements, processes, and procedures) that is based on recognized cyber security methodologies, standards, or best practices?

Question #	SVA Question
[Q:14.4-2855]	Risk and Vulnerability Management: Are network and system (application) level security tests performed (vulnerability scans, penetration tests, open communication line scans, authorized hardware and software scans) on a regular basis; and after configuration changes or being patched or upgraded - before being put into operation?
[Q:14.4-2856]	Risk and Vulnerability Management: Has the facility incorporated the vulnerability solutions that are applicable and appropriate for the environment (e.g., are firewalls configured for minimum business or operational needs)?

After you answer all of the questions about the asset's cyber control system, select the check box next to **Cyber Control System Complete**. You will then be returned to the **Cyber Control System** screen to provide information for any additional cyber control systems. When you are finished providing information, answer the question at the bottom of the screen, "Have all cyber control systems been evaluated?" Select Yes and click the [Next] button to continue.

8.2 Business Control Systems

If you identified any business control system earlier in the SVA, the **Business Control System** screen will be shown. You will need to answer the series of questions by selecting **Describe <Business Control System Name>** for each business control system listed. This section begins with the following question:

Question #	SVA Question	Question Details
[Q:14.61-4175]	Is this cyber system physically located at the facility?	Provide a Yes or No answer for this question. • If the answer is Yes, you will be asked to map the system's location. • If the answer is No, you will be asked to identify where the system is located.

8.2.1 Mapping Business Control System

The **Business Control Location** screen allows you to identify the location of the asset's business control system on an interactive aerial map of the facility and its immediate surrounding area. There are two primary features to assist the user with map navigation: the map tool bar and the associated map help table, which provides information on how to use the map tool bar.

- The map tool bar features the following functions:
 - o **Panning:** Click the [Pan] button to navigate within the map to find the business control system. After clicking [Pan], place your pointer within the map display area, hold down your left mouse button, and drag the map to the desired location. Click the [Pan] button again to deactivate the pan function.
 - o **Zooming In:** Click the [Zoom In] button to increase the magnification of the map display area where the business control system is located. After clicking the [Zoom In] button, place your pointer near the place within the map display area you would like to magnify. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be magnified. You can continue to use this method to zoom to the level of magnification that is sufficient for locating the business control system. Click the [Zoom In] button again to deactivate the magnification function.
 - o **Zooming Out:** Click the [Zoom Out] button if additional adjustment to the map display area is necessary to allow for a wider view. After clicking the [Zoom Out] button, place your pointer near the place within the map display area you would like to contract. Hold down your left mouse button, and drag the pointer to form a red box around the specific location that needs to be contracted. Click the [Zoom Out] button again to deactivate the contraction function.
 - o **Full Extent:** Click the [Full Extent] button to reset the map to its fullest view. Repeat the steps described above until the business control system is clearly identified.
 - o **Locate System:** Click the [Locate System] to pinpoint the location of the business control system on the map. Clicking the [Locate System] button will allow you to use your pointer to place a visible identifier, a pink star ★, on the map at the business control system location. Click the [Locate System] button again to deactivate the location function.

Once you are satisfied that the business control system has been located and that you have successfully placed an image of the business control system within the map display area, click the [Next] button at the bottom of the screen. **NOTE:** Do **not** click the [Next] button until you place the pink star on the map.

8.2.2 Locating Offsite Business Systems

If the business control system is not located at the asset's facility, you will need to answer the following questions:

Question #	SVA Question	Question Details
[Q:14.62-8232]	Select the Country	Use the provided drop-down list box to identify the country in which the business control system is located.
[Q:14.63-4177]	Location/Building Name	Provided the required information in the data field provided.
[Q:14.63-4178]	Street	Provided the required information in the data field provided.
[Q:14.63-8271]	Street Line 2	Provided the required information in the data field provided.
[Q:14.63-4179]	City	Provided the required information in the data field provided.
[Q:14.63-4180]	State	Provided the required information in the data field provided.
[Q:14.63-4181]	ZIP Code	Provided the required information in the data field provided.

8.2.3 Business System Questions

The following table lists the questions that you will need to answer about the asset's business control system. Provide a Yes or No answer for each question.

Question #	SVA Question
[Q:14.8-1033]	Is external access (e.g., Internet, modem, wireless) to cyber systems allowed?
[Q:14.81-1034]	Has the lack of external access been validated through testing by IT security professional services?
[Q:14.82-1035]	Are the capabilities of the cyber systems limited in the facility in regard to communications with portable cyber equipment (authorized or not) (e.g., laptop computers, personal digital assistants (PDAs), flash drives, data disks, smart cell phones)?
[Q:14.83-1036]	Has the disabling of communication capabilities been validated through testing by a professional IT security service?

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question
[Q:14.84-1051]	Security Policy: Does the facility have documented and distributed cyber security policies, plans, and supporting procedures commensurate with the current information technology operating environment?
[Q: 14.84-1071]	Security Policy: Does the facility have a documented and distributed cyber change management policy and supporting procedures (e.g., new hardware/software, employee access)?
[Q: 14.84-1072]	Security Policy: Has an individual(s) been designated as responsible for cyber security at the facility?
[Q: 14.84-2811]	Access Control: Does the facility allow systems to have external connections with portable electronic devices configured for minimum business needs and verified with scans?
[Q: 14.84-1092]	Access Control: Does the facility practice the concept of least privilege (e.g., users are only granted access to those files and applications based on role and responsibilities)?
[Q: 14.84-1093]	Access Control: Have all default passwords been changed to user-specific passwords?
[Q: 14.84-1094]	Access Control: Are accounts locked out after several unsuccessful login attempts?
[Q: 14.85-1100]	Personnel Security: Does the facility perform background checks for personnel in critical/sensitive positions?
[Q:14.85-1101]	Personnel Security: Does the facility actively maintain the access control list to ensure that all cyber system accounts are modified, deleted, or de-activated as personnel leave the company or transfer into new roles?
[Q:14.85-1105]	Physical and Environmental: Does the facility restrict physical access to sensitive or restricted IT, telecommunications, media storage, and control areas to those with appropriate need?
[Q:14.85-1107]	Awareness and Training: Does the facility provide cyber security training?
[Q: 14.86-1151]	Monitoring and Incident Response: Does the facility log cyber security events on systems and review them on a regular basis?
[Q:14.86-2831]	Monitoring and Incident Response: Does the facility log cyber security events on servers, and review them on a regular basis?
[Q: 14.86-1152]	Monitoring and Incident Response: Does the facility report significant cyber security events to senior management?
[Q 14.86-1153]	Monitoring and Incident Response: Does the facility mandate malicious code protection on all systems?
[Q: 14.87-1173]	Monitoring and Incident Response: Does the cyber system allow email?
[Q: 14.88-1174]	Monitoring and Incident Response: Are email attachments (e.g., executable files) filtered on incoming email?

CSAT Security Vulnerability Assessment Application Instructions

Question #	SVA Question
[Q: 14.9-1191]	Configuration Management: Has a business requirement been established for every external connection into the network/ environment, including wireless and modem connections?
[Q: 14.9-1192]	Configuration Management: Does the facility apply/perform regular software and hardware, patches, updates, upgrades, and replacements?
[Q: 14.9-1193]	Configuration Management: Are configuration changes to the network and application's hardware and software reviewed by an IT security professional and by management to assess the security impact prior to the changes being implemented to the operational environment?
[Q: 14.9-2832]	Risk and Vulnerability Management: Have potential vulnerabilities of critical assets, systems, and networks been identified and evaluated?
[Q: 14.9-1195]	Risk and Vulnerability Management: Does the facility have a means to identify and measure cyber security risk (including requirements, processes, and procedures) that is based on recognized cyber security methodologies, standards, or best practices?
[Q: 14.9-2833]	Risk and Vulnerability Management: Are network and system (application) level security tests performed (vulnerability scans, penetration tests, open communication line scans, authorized hardware and software scans) on a regular basis; and after configuration changes or being patched or upgraded - before being put into operation?
[Q: 14.9-2834]	Risk and Vulnerability Management: Has the facility incorporated the vulnerability solutions that are applicable and appropriate for the environment (e.g., are firewalls configured for minimum business or operational needs)?

After you answer all of the questions about the asset's business control system, select the check box next to **Business Control System Complete**. You will then be returned to the **Business Control System** screen to provide information for any additional business control systems. When you are finished providing information, answer the question at the bottom of the screen, "Have all business control systems been evaluated?" Select Yes and click the [Next] button to continue.

When you are finished answering all the computer security analysis questions, answer the question at the bottom of the screen, "Have all Computer Security Analysis questions been completed?" Select Yes and click the [Next] button to continue.

9. SVA Completion

After entering all of the relevant data, you will see the **SVA Completion** screen. The **SVA Completion** screen will prompt you to both validate the information you entered and review it for completeness and accuracy before final submission.

General Survey Completion 81%

< Back Save Next >

SVA Completion

Submission Statement:

My statements in this submission are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Based on the information supplied, the Laura's Demo Facility 2 may be covered by the Department of Homeland Security under Section 550 of the Homeland Security Appropriations Act of 2007. You will be mailed a letter that will identify your facility's regulatory status. If you are regulated it will indicate the final tier of Laura's Demo Facility 2 and specific security issues that need to be addressed in the SSP required under Section 550.

Press the **Next** button to continue the submittal process. You will have an opportunity to validate and print your survey before it is submitted to DHS.

< Back Save Next >

Picture 9.1: SVA Completion Screen

9.1 Validating Reports

A validation check for basic logical errors can be done at any time by selecting the **Validate Report** command on the **SVA Survey Navigation Menu** on the left side of the screen. Information that is missing or incorrectly formatted will be listed and highlighted in red, and a link will be provided to take you to the affected area to fix the error or add the missing information. Once the information has been corrected, select the **Validate Report** command again to check for any additional errors.

NOTE: The SVA application will *not* find and display errors other than missing required data or logical errors (e.g., unrecognized characters such as commas or percent signs). Even if no validation errors appear when the **Validation Report** command is selected, you are encouraged to print a copy of the SVA Summary Report and review it for accuracy.

9.2 Summary Reports

Select the [View Summary Report](#) command on the **SVA Survey Navigation Menu** on the left side of the screen to generate a report that lists the SVA questions and the data entered for each. Depending on the size of your survey, this job is sometimes run in the background, so you can continue to work while this report is generated. If this happens, you will get an email when the report is complete. Once generated, the report will also be available from the **CSAT Survey List** Screen, but only until submission. This report can be printed, either by clicking the [Print this Report](#) command on the top of the screen, or by using the print function in your browser. **NOTE:** The printed or electronic SVA record is CVI, and it *must* be protected as CVI.

Print This
Report
Command

Homeland Security | Chemical Security Assessment Tool (CSAT) | OMB No: 1670-0007 | Expiration Date: March 1, 2011
Security Vulnerability Assessment (SVA) | Chemical-terrorism Vulnerability Information (CTVI)

[Print this Report](#)

Summary Report

General

Submission Statement:

My statements in this submission are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Enter the facility identification number from the DHS Preliminary Tier Determination Letter.
[0-10-3311]

1111

Picture 9.2: SVA Summary Report Screen

When the SVA Summary Report has been successfully reviewed and validated, click the [Next] button to continue the completion process.

NOTE: If the Preparer of the SVA is also its Submitter and has only one user name, the screen display will be similar to the Submitter screens in the next few sections. The Preparer will *not* have the option to transfer the account to the Submitter, but will be directed to submit the completed SVA directly to DHS.

9.3 Transferring to Submitter

Click the [Transfer to Submitter for Review] button to transmit the SVA to the Submitter for review. Once the SVA is sent to the Submitter, the Preparer has read-only access to the data unless the Submitter sends the SVA back for revisions, including the entry of additional data.

The Preparer can also choose to have a copy of e-mail communications from DHS sent to them as well by answering Yes to the question, “Do you want a copy of the letter with the final tiering to be sent to the Preparer in addition to the Submitter?”

Picture 9.3: DHS Communications/Preparer Copy Screen

9.4 Submitter Review

After the Preparer has submitted the completed SVA, the Submitter will receive an e-mail notifying him/her that the SVA is ready for review. On the **CSAT Survey List** screen (see Picture 3.1), the Submitter will see the facility (or list of facilities) he/she is authorized to review and the facility's status in the review process. Surveys that are awaiting final review and submission will have the status of **In Review**.

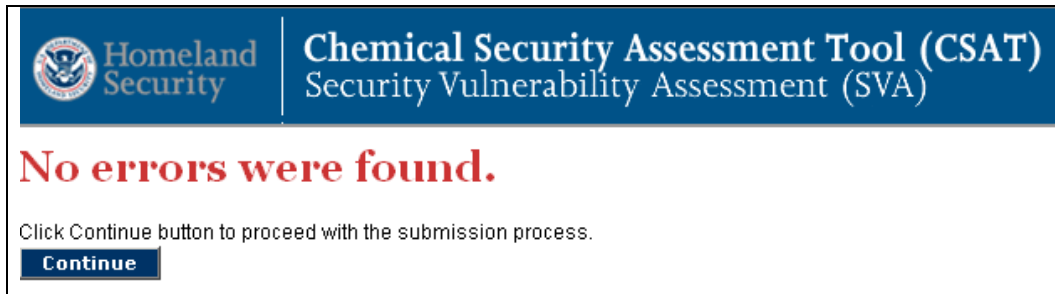
The Submitter will select the name of the facility to review, and look through the SVA to view and edit the answers supplied by the Preparer. After reviewing all of the information, the **Completion** screen will be displayed and the Submitter can either:

- Return the survey to the Preparer for edits and/or additions by clicking the [Transfer to Preparer for Modifications] button; or
- Proceed to the **Final Validation** screen by clicking the [Final Validation] button.

NOTE: If the SVA is returned to the Preparer, its status will return to **In Progress** on the **CSAT Survey List** screen and the Preparer and Submitter will receive e-mails with additional instructions.

Picture 9.4: Submitter Review Buttons

To finish the SVA, the Submitter will click the [Final Validation] button and correct any errors or omissions. When the validation is complete, the Submitter will click the [Continue] button.



Picture 9.5: Validation Complete Screen

NOTE: The Submitter *must* retain a copy of the completed SVA for the facility's records, as specified in 6 CFR §27.255(b). Once the SVA is submitted to DHS, a facility no longer has access to it; thus, a copy of the submitted SVA will be helpful in case the data needs to be re-entered. You can create a copy of the completed SVA by selecting the [Print Version of SVA](#) command on the **SVA Finish** screen. After printing a copy for the file and verifying that the copy is legible; the Submitter should click the [Submit to DHS] button on the **SVA Finish** screen to officially submit the completed SVA.

Picture 9.6: SVA Finish Screen

After receiving the submitted SVA (or ASP, if applicable), DHS will evaluate the submission to determine whether the facility is still considered high-risk and, if so, to assign a final tier determination. DHS will notify the facility in writing of its final tier determination and provide further information and instructions for the facility to develop and submit an SSP.

Appendix A: Acronyms Reference List

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 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	U.S. 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
PCS	Process Control Systems
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