CSAT Security Vulnerability Assessment

Instructions

June 2008

Version 1.0

Homeland Security

Table of Contents

Note to Users 1
Introduction 2
SVA Instructions: The SVA Process 2
Organization of these Instructions 3
CSAT User Access Roles 4
Preparing to Complete the SVA: Relevant Information and Resources 4
Getting Additional Help 5
Chemical-terrorism Vulnerability Information 5
1.0 Getting Started 6
1.1 Sign-in Screen 6
1.1.1 Add Reviewer 6
1.1.2 Update Facility Information 7
1.2 Navigating within the Tool 8
1.2.1 Saving the Data 10
1.2.2 Validating Data 10
1.3 Pre-population from Top-Screen 11
2.0 General Facility Information 13
2.1 Facility Map 14
2.2 Tier 4 Status 15
2.2.1 ASP Documents 16
2.2.2 Upload ASP Documents 17
2.2.3 Plot Plans/Maps 19
2.2.4 Map Image Details 19
2.2.5 ASP Submission 19
2.2.6 Completion 20
3.0 Facility Security Issues 21
3.1 Reporting Facility Security Issues 21
3.2 Reporting Chemicals of Interest 23
3.3 Summary of Facility Security Issues 24
3.4 Facility Characteristics 25
3.5 Facility Security Information 26
3.5.1 Security Equipment at the Facility 26
3.5.2 Additional Security Equipment 28
3.5.3 Utility Systems and Infrastructure Support 28
3.5.4 Additional Utility Systems 29
3.5.5 Inventory Control Measures 29
3.5.6 Personnel Access Control Measure 33
3.5.7 Additional Personnel Access Controls 34
3.5.8 Shipping and Receiving Control Measures 34
3.5.9 Post-release Measures and Equipment 35
3.5.10 Additional Post-release Measures 36
3.5.11 Site Vulnerability Factors 36
4.0 Asset Characterization 38
4.1 Identifying Assets 38
4.2 Characterize Assets 41
4.2.1 COI Associated with Asset 44

4.2.2 Detailed COI Information for Asset 45
4.2.3 Initial Identification of Cyber Control and Business Systems: 53
4.2.4 Asset Complete 54
4.3 Cyber Control Systems 55
4.4 Cyber Business Systems 56
5.0 Vulnerability Analysis 57
5.1 Summary of Facility Vulnerability 57
5.2 Facility Security Issues to Be Analyzed 57
5.3 Introduction Screen 58
5.4 Asset Location 58
5.5 Attack Mode Screen 60
5.5.1 Select Attack Scenario 62
5.5.2 Attack Location Map 65
5.5.3 Attack Scenario Questions 67
5.5.4 Vulnerability Factors Questions 67
5.5.5 Release Questions 75
5.5.6 Vulnerability Analysis Complete 76
6.0 Computer Systems Analysis 77
6.1 Cyber Control Systems 77
6.1.1 Map Cyber Control System 77
6.1.2 Cyber Control System Questions 77
6.2 Business Control Systems 80
6.2.1 Map Business Control System 80
6.2.2 Locate Business System Not at Asset 81
6.2.3 Business System Questions 81
7.0 SVA Completion 84
List of Acronyms 89

Note to Users

This document provides instructions to facilities for completing and submitting the Chemical Security Assessment Tool (CSAT) Security Vulnerability Assessment (SVA) in accordance with requirements of the Department of Homeland Security's (DHS's) Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27.

The CFATS rule authorizes DHS to collect information from chemical facilities on a broad range of topics related to the potential consequences of, or vulnerabilities to, a terrorist attack or incident. The CSAT SVA is one method DHS uses, as provided by 6 CFR § 27.215, to gather such information from high-risk facilities. Certain high-risk facilities may choose to submit an Alternative Security Program (ASP) in lieu of an SVA, as provided by 6 CFR § 27.235. This document also provides instructions on submitting an ASP for those facilities authorized to do so.

All examples in these instructions are illustrative and intended to highlight a specific point. Each facility must carefully consider the unique characteristics and circumstances of its own facility to determine the relevance and appropriateness of each example.

CSAT users may call the CSAT Help Desk with questions regarding the CSAT SVA Tool. The CSAT Help Desk can be reached at 866-323-2957 between 7 a.m. and 7 p.m. (Eastern time), Monday through Friday. The CSAT Help Desk is closed for Federal holidays.

Introduction

Section 550 of the DHS Appropriations Act of 2007, Pub L. 109-295 (Sec. 550 or the Act), authorizes DHS to regulate the security of high-risk chemical facilities. The Chemical Facility Anti-Terrorism Standards (CFATS) Interim Final Rule (IFR), 6 CFR Part 27, was published on April 9, 2007, to implement the Act.

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

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

Following submission of the SVA and analysis by DHS, 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. For facilities confirmed to be high-risk, DHS will also communicate the final facility tier determination, after which the facility must complete a Site Security Plan (SSP) under 6 CFR § 27.225 or, alternatively, the facility may choose to submit an ASP in lieu of an SSP, as provided by 6 CFR § 235.

These Instructions apply only to the CSAT SVA tool, which includes a process for submitting ASPs where appropriate.

SVA Instructions: The SVA Process

The CSAT SVA follows a logical data collection process. First, it collects basic facility identification information. Second, it collects information about the chemicals that a facility possesses. Third, it collects information about assets at the facility that involve the chemicals of interest identified by DHS in the DHS initial notification letter. The tool then enables the users to locate assets on an interactive map and requires that the user apply DHS attack scenarios, or define attack scenarios of its own to run against its assets, which provides DHS with data on the vulnerability and consequentiality of such attacks. The user assesses the vulnerability of the facility based, in part, on the security measures already in place at the facility. Finally, the SVA collects information on relevant cyber systems that may affect the security of identified assets.

Organization of these Instructions

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

The Introduction provides a brief overview of CFATS and the CSAT SVA process, the organizational structure of these Instructions, CSAT user access roles, a listing of information that may be helpful in completing the SVA tool, and resources for getting additional help in completing the SVA tool.

Section 1 covers Getting Started.
This includes signing into the SVA, instructions on navigating the SVA and saving and validating your data.

Section 2 covers General Facility Information.
This includes facility name, address and mapping the location.

Section 3 covers Facility Security Issues.
This includes identifying security issues and Chemicals of Interest (COI) listed in the DHS initial notification letter.

Section 4 covers Asset Characterization.
This includes identifying assets at the facility and providing information about the asset, including where the asset is located and which COI are associated with the asset.

Section 5 covers Vulnerability Analysis.
This includes providing attack scenarios, vulnerability factors and release scenario information for the assets defined by the user in the Asset Characterization section.

Section 6 covers Computer Systems Analysis.
This includes identifying and answering questions about cyber control and business control systems associated with the assets.

Section 7 discusses validating, reviewing, and submitting the SVA to DHS.

For easy identification of questions, the question number appears in brackets in the text of these Instructions as well as in the SVA tool. For example, "[Q:1.0-3311]" appears below the question

requesting the Facility Name. This question number also appears in the associated explanation in these Instructions. The question number is also a handy reference if a user contacts the CSAT Help Desk.[1]

CSAT User Access Roles

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

For each facility, a variety of individuals can be authorized to use CSAT. Each registered individual will be assigned a specific role, with access rights and privileges based on that role unless roles are transferred as indicated below. The roles (Preparer, Submitter, Authorizer, and Reviewer) are defined in the CSAT User Registration Guide. Facilities may assign and/or transfer responsibility among individuals through the CSAT system. Information on how to assign and/or transfer or consolidate accounts is available in the CSAT User Registration Guide and Account Management Guide available at http://www.dhs.gov/xprevprot/programs/gc_1169501486197.shtm

It is important to note that when the Preparer sends the SVA to the Submitter for review, the Preparer will no longer be able to edit the information unless the SVA is returned to the Preparer by the Submitter for revision. If the Submitter returns the SVA to the Preparer for changes, the Preparer will once again be able to edit the SVA information before returning it to the Submitter for submission to DHS. When the Submitter has access to the SVA, the information may be revised by the Submitter. Once the Submitter transmits the information to DHS, it is no longer accessible to the facility or its designated Preparer, Authorizer, Reviewer, and/or Submitter. The Authorizer has no role in the on-line review of the SVA unless he or she is also the Preparer or Submitter. If an 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. Therefore, the facility should retain a copy of its completed SVA. See Section 7 for directions on how to print out a copy of the SVA before it is submitted to DHS.

Preparing to Complete the SVA: Relevant Information and Resources

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

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

[1] The CSAT Help Desk has a toll-free number that CSAT users can call with questions regarding CSAT. 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 for Federal holidays.

- A copy of the Chemical-terrorism Vulnerability Information (CVI) Procedural Manual regarding protection of CVI, available at http://www.dhs.gov/chemicalsecurity.
- A copy of the DHS initial notification letter that was sent to the facility notifying the facility of its initial status as a high-risk chemical facility, assigning a preliminary tier and listing the chemicals of interest that DHS has determined 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, available at csat.dhs.gov/csat.
- Chemical inventory information, including the names and quantities of all DHS COI that 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 that may have been completed by the facility.

Getting Additional Help

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

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

Chemical-terrorism Vulnerability Information

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

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 CVI and the protection of chemical facility security information, please refer to the CVI Procedures Manual, which is available at http://www.dhs.gov/chemicalsecurity.

1.0 Getting Started

1.1 Sign-in Screen

The DHS initial notification letter sent to the facility by DHS will have instructions for accessing the CSAT SVA tool. The user will be prompted for their username and password.

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

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

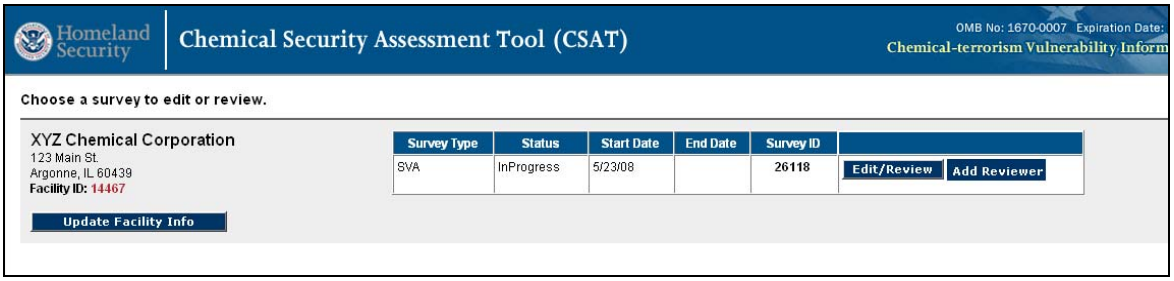

Figure 1-1 – Choose Facility

1.1.1 Add Reviewer

At this point, 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 for that same facility. To add a Reviewer, click on the *Add Reviewer* button below the facility name for which you would like to add the Reviewer. After clicking the *Add Reviewer* button, the user will be directed to a screen asking whether the user would like to grant Reviewer access to an existing CSAT User or a new CSAT User. Select the appropriate choice by clicking on the blue bar and entering the requested information.

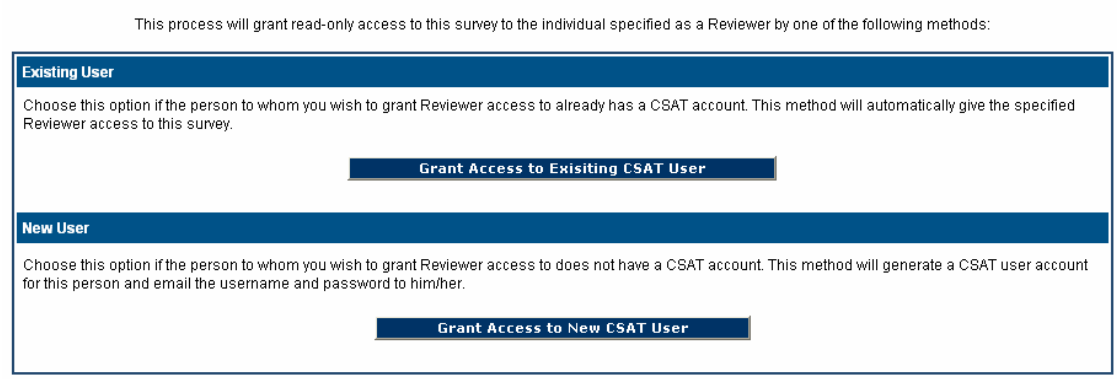

Figure 1-2 – Granting Reviewer Access

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

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

1.1.2 Update Facility Information

To update facility information, including changing the name or address, click on the *Update Facility Info* button.

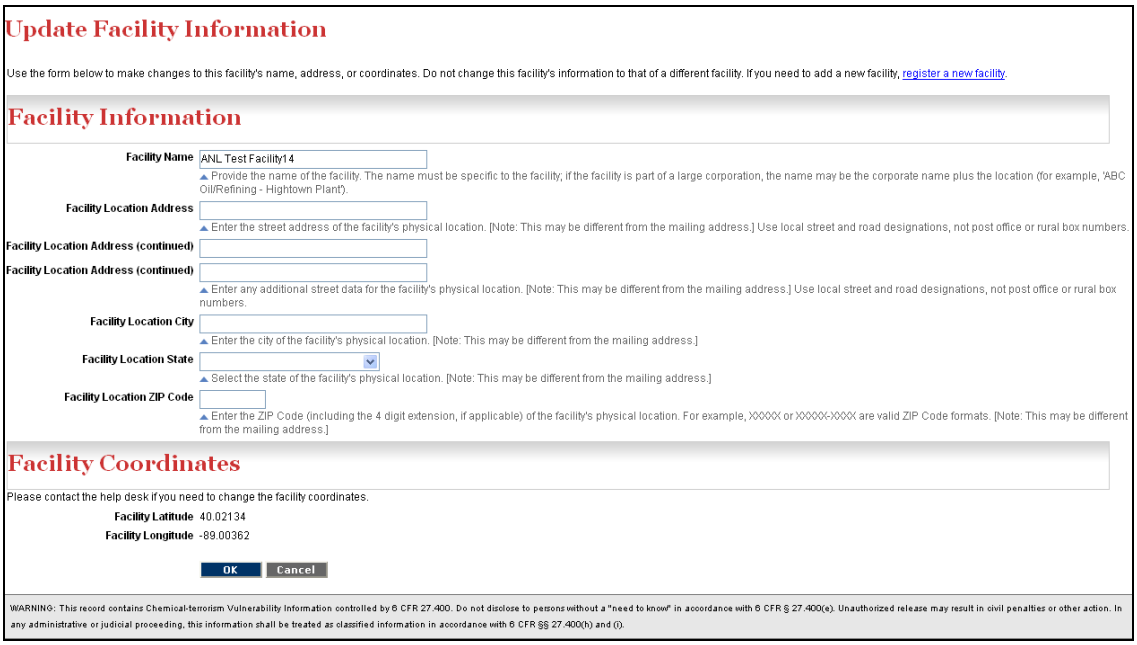

Figure 1-3 – Update Facility Information

Basic facility information can be updated. Do not use this screen to create a new facility. If a new facility needs to registered, click the *register a new facility* text at the top of the screen. Enter any corrections in the

appropriate boxes and click OK. A facility's coordinates (Latitude/Longitude) cannot be changed from within the SVA application. Contact the Help Desk to process a lat/long change.

1.2 Navigating within the Tool

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

Figure 1-4 – SVA Back and Next Buttons

Using the ***Next*** and ***Back*** buttons will automatically save the information that was entered on the page.

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

A navigational menu appears on the left side of the screen (see Figure 1-5). Users can also navigate through the SVA by clicking on the desired topic in that menu. The descriptions of the sections of the SVA will be highlighted once the General Section of the SVA has been completed. **Please note that if a user returns to a section of the SVA that was previously completed, all the subsequent pages need to be reviewed** (using the *Next* button on each page). This is required because the system adapts the pages presented for completion based on answers on previous pages. A change within a section might require the user to answer additional/different questions later.

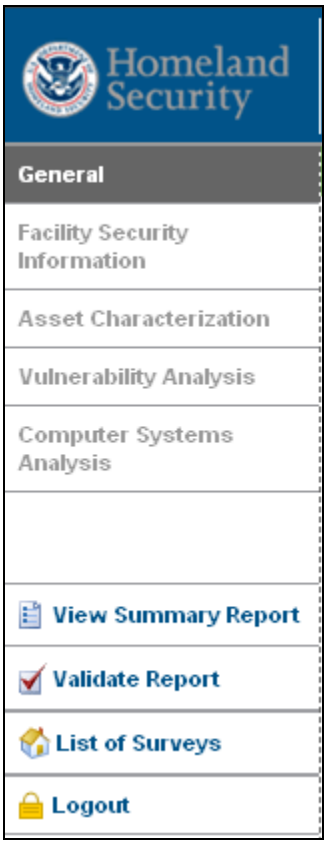

Figure 1-5 – SVA Navigational Menu

On some screens, additional rows of text will need to be added to complete the response to a question. When more than one text field is needed, use the ***Add*** button to add a row. The ***Delete*** button can be used to delete a row or an entry.

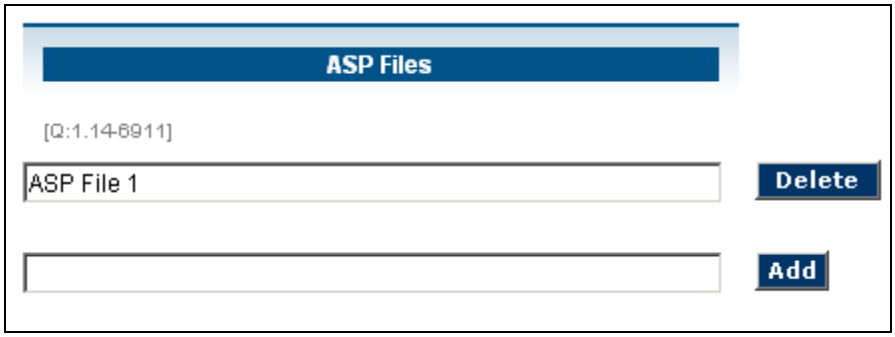

Figure 1-6 – SVA Add Button

Where further explanation of a response is required, a *Describe* button is provided. When a *Describe* button appears, click it to answer additional questions specific to that item. At the conclusion of these additional questions, the user will be asked if the description is complete (a check box). When the user indicates that the questions are complete, they will return to the list of items. If the user marked the item complete and all required questions were answered for that item, the item will be displayed with a green check mark

icon. If the user does not check the box to indicate that the questions are complete, or if any required questions were not answered, the item will be displayed with a yellow warning icon as a reminder that the item is incomplete. Figure 1-7 shows both a complete and incomplete icon.

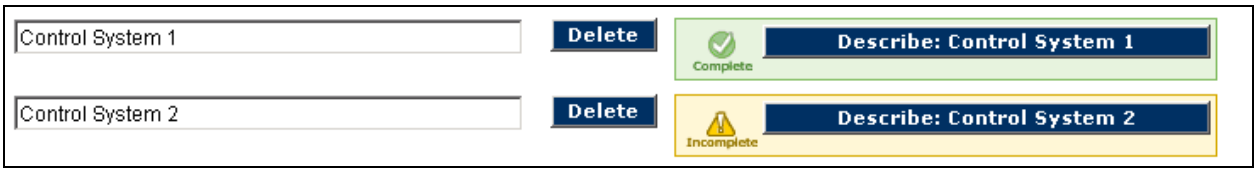

Figure 1-7 – SVA Describe Button

The user's session will "time out" after 20 minutes if the system is not in use. Users will need to log back in to restart the session. Data that have been entered and saved by clicking the ***Next*** button will not be lost and the session will reopen on the same screen where the session "timed out."

1.2.1 Saving the Data

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

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

1.2.2 Validating Data

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

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

Using the *Validate Report* option on the navigation menu will provide a more complete validation check. A validation error message will be displayed if required data input fields are skipped or completed incorrectly. The system allows the user to return to the error and correct it. For example, if the name of the facility is not entered, the following error report will be displayed. (See Figure 1-8). The link will direct the user to the input area for correction.

Validation is done for logic and basic errors only. Accordingly, the validation function should not be relied upon to ensure the SVA has been completed without errors. The Submitter is responsible for submitting accurate and correct information to the best of his or her knowledge.

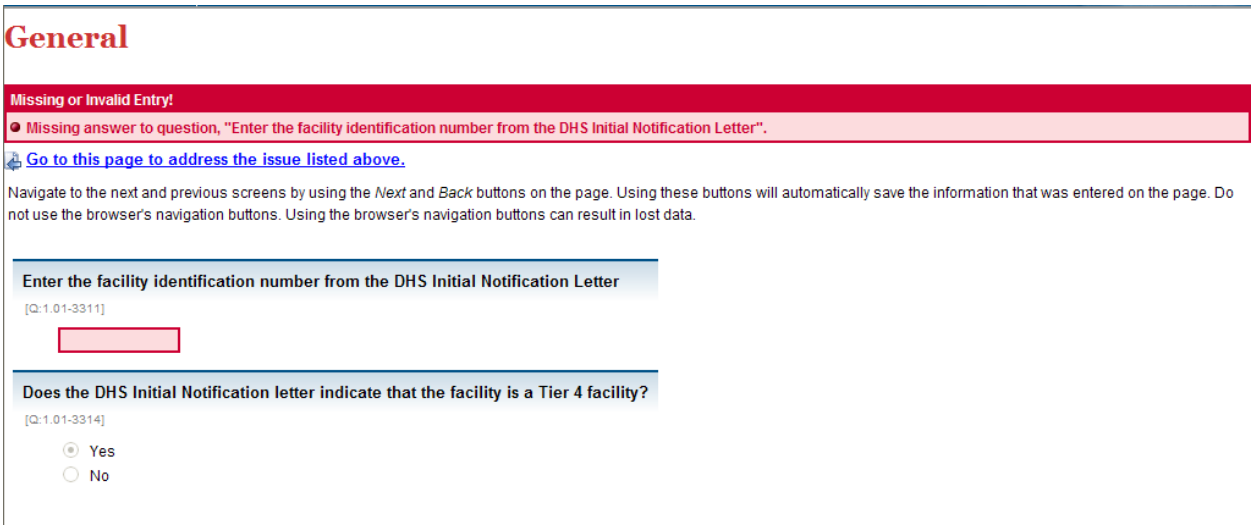

Figure 1-8 – Error Report Screen

1.3 Pre-population from Top-Screen

For consistency, the following questions may be pre-populated from the CSAT Top-Screen and some responses will not be editable or, in some cases, even viewable. 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. If those answers are no longer correct, please contact the Help Desk. In some cases, pre-population cannot be completed and the user will be required to answer the following questions.

Questions that may be pre-populated from the CSAT Top-Screen:

- [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?

2.0 General Facility Information

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

- The information requested in this section can be found in the DHS initial notification letter. A screen shot from the SVA appears below.

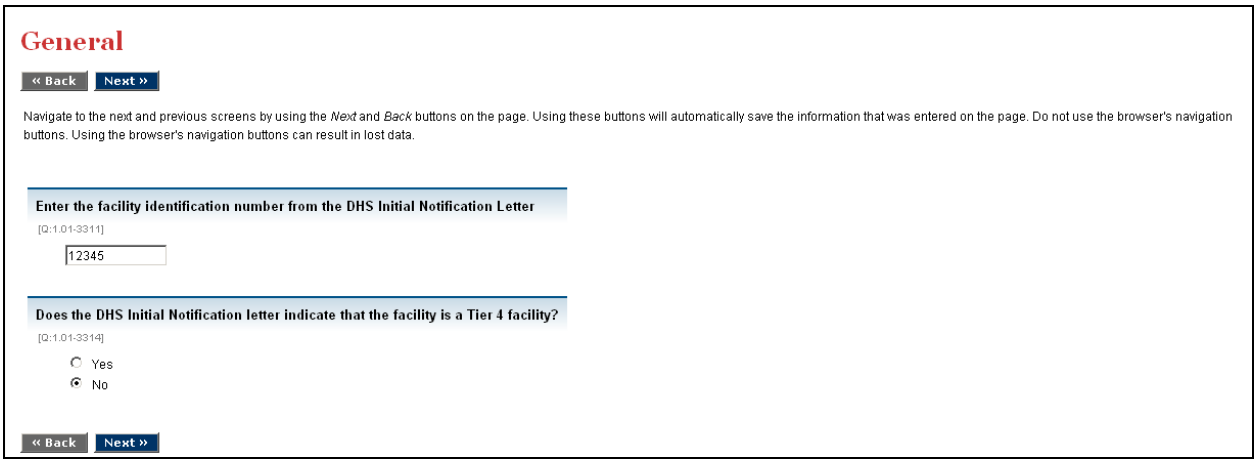

Figure 2-1 General SVA Screen

Facility Identification Number. [Q:1.0-3311] 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 Figure 1.1.

Facility Tier Level. [Q:1.0-3314] 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 Alternative Security Program (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 and should complete the CSAT SVA and select *No* to answer this question.

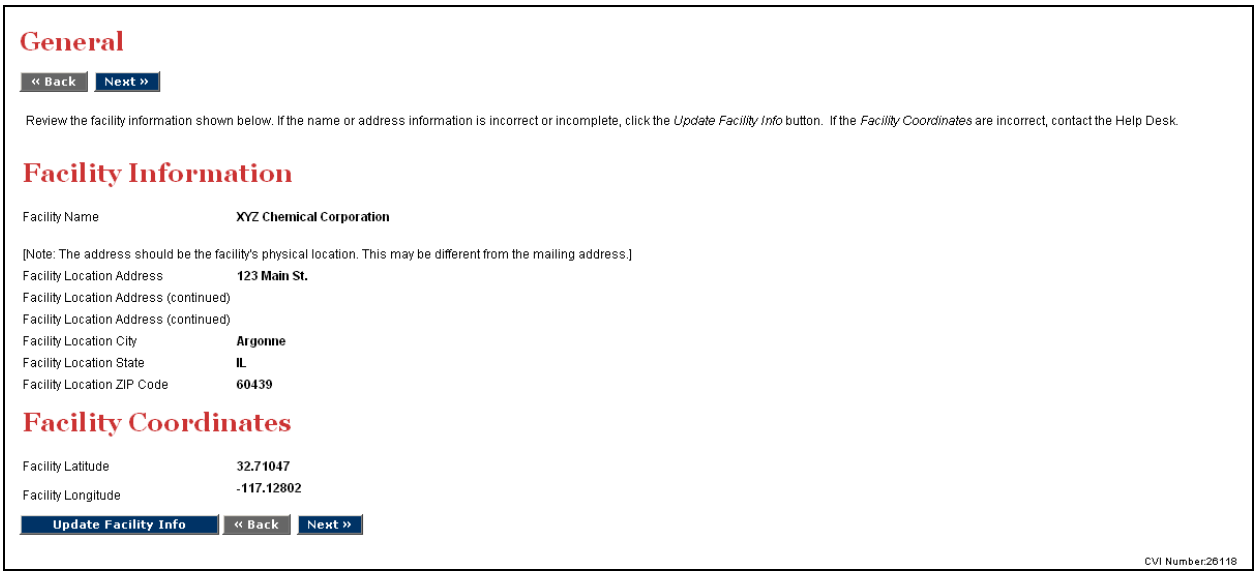

Figure 2-2 Facility Name and Address SVA Screen

Facility Name and location will be completed from the Top-Screen. If this information needs to be updated, click the *Update Facility Info* button and make changes. Latitude and longitude cannot be changed; contact the Help Desk to modify incorrect latitude or longitude.

2.1 Facility Map

The Facility Map allows the user to identify the location of the facility on an interactive aerial map of the subject facility and the immediate surrounding area.

The user should familiarize themselves with the map navigation features prior to locating the facility. There are two primary features to assist the user with map navigation: the Map Tool Bar and the associated Map Help table.

Zoom In	Zoom Out	Pan	Full Extent

Figure 2-3 – Map Tool Bar to View Facility Map

The user may need to navigate within the map to find the facility by using the *Pan* function. This is accomplished by clicking on *Pan* and then engaging the directional function by clicking on the map and "dragging" to the desired area.

When the user has located the general area containing the facility, increased magnification is usually required. Increase magnification by clicking on the *Zoom In* button and then click and hold the left mouse button while dragging the cursor to form a red box around the specific area that needs to be magnified. The user can continue to use this method to zoom to the level of magnification that is sufficient for locating the facility.

If additional adjustment is necessary, the *Zoom Out* button allows the user to click and drag to a wider localized view. If resetting the full map is desired, simply click the *Full Extent* button to provide the widest view possible and repeat the steps described above until the asset is clearly identified.

Map Help	
Click a button in the map toolbar to choose a tool. The tools may be used as follows:	
Zoom In	Click and drag to create a rectangle around the area that you want to magnify.
Zoom Out	Click and drag to zoom out.
Pan	Click and drag to view other parts of the map without resizing. The map will move in the direction the user drags.
Full Extent	Click the *Full Extent* button once to view the magnification that shows the entire map. At the full extent, the user will not be able to zoom out further.

Figure 2-4 – Map Help Table

Once the user is satisfied that the facility has been located, and fills most of the screen with the site image, click on the *Next* button.

If the facility cannot be located, or the image does not provide adequate detail and the user has a better map, click on the *Upload Facility Map* button. The user will be prompted to supply the new map. The user then clicks on the *Next* button to continue.

All Tier 4 facilities will be directed to another screen which will provide the option to upload an Alternate Security Program (ASP) in lieu of an SVA. Further explanation is included in the Tier 4 Status section below. 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.

2.2 Tier 4 Status

CFATS provides Tier 4 facilities with the option of submitting an SVA using the CSAT SVA or submitting an ASP in place of the SVA. DHS may approve an ASP in whole or in part, or subject to revision or supplements, if the ASP meets the requirements of CFATS and provides for an equivalent level of security. If a Tier 4 facility elects to submit an ASP, rather than submit the CSAT SVA, this section describes the process to upload the relevant ASP files into the CSAT SVA tool. 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 will be asked to answer *Yes* or *No* to the following question.

Alternate Security Program [Q:1.01-3315] Do you want to upload an Alternate Security Program (ASP)? If the user plans to upload an ASP and not complete the CSAT SVA, answer *Yes*, and follow the remaining instructions on uploading an ASP to DHS. If the user does not plan to upload an ASP, select *No*, and the user will be prompted to complete the CSAT SVA, beginning with the next step, **Facility Security Issues**.

2.2.1 ASP Documents

Before uploading an ASP, the user will be asked questions related to the factors (see 6 CFR §§ 27.215, 27.235) for submitting an ASP in lieu of an SVA or otherwise relevant to the Department's determination of whether to approve the ASP. If the user answers *No* to any of these questions, the user will user 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. [Q:1.12-12451]

SVA Scope (Issues and Chemicals of Interest). [Q:1.1-3316] 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 a facility answers *Yes* to this question, it is confirming that the ASP covers all chemicals of interest (COI) above the threshold quantities detailed in Appendix A to CFATS, as well as all applicable security issues identified in the initial notification letter, i.e.,:

- Release of toxic, flammable or explosive COI and/or
- Theft/diversion of COI and/or
- Sabotage/contamination of a COI

Does the ASP use a Center for Chemical Process Safety (CCPS)-approved methodology? [Q:1.1-11671]

Does the ASP address the *asset characterization* factors described in 6 CFR 27.215? [Q:1.1-11672] Asset Characterization includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection.

Does the ASP address the *threat assessment* factors described in 6 CFR 27.215? [Q:1.1-11673] Threat assessment includes a description of possible internal threats, external threats, and internally-assisted threats.

Does the ASP cover all of the applicable attack modes included in the CSAT SVA? [Q:1.1-3317] When a facility answers *Yes* to this question, they 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/csat to active CSAT users that have completed CVI training and have started their SVA.

- Vehicle Borne Improvised Explosive Device (VBIED)
- Maritime
- Aircraft
- Theft
- Diversion
- Sabotage
- Assault Team
- Standoff

Does the ASP address the *countermeasures* factors described in 6 CFR 27.215? [Q:1.1-11674] Security vulnerability analysis includes the identification of potential security vulnerabilities and the identification of

existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards.

Does the ASP address the *risk assessment* factors described in 6 CFR 27.215? [Q:1.1-11675] 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 the likelihood of the success of an attack.

Tier 4 facilities that choose to upload an ASP in lieu of the CSAT SVA also must provide the name of any (non-CSAT) security vulnerability assessment methodology previously performed and used in the ASP that is being uploaded and the date the non-CSAT security vulnerability assessment was completed.

Click *Next* to move to next screen.

Non-CSAT Security Vulnerability Assessment Methodology. [Q:1.13-3320] Enter the name of the non-CSAT security vulnerability methodology. For Tier 4 facilities uploading an ASP in lieu of an SVA, the name of the non-CSAT Security Vulnerability Assessment methodology that is being uploaded should be entered in the text box under the question number.

Date of Non-CSAT Security Vulnerability Assessment. [Q:1.13-3331] What is the date of the non-CSAT security vulnerability assessment? Use the following date format mm/dd/yyyy (e.g., May 1, 2006 is entered as 05/01/2006).

2.2.2 Upload ASP Documents

For a Tier 4 facility that elects to upload an ASP in lieu of an SVA after answering the questions described in Section 2.2.1, this section describes the steps for uploading the ASP documents to DHS through the CSAT SVA tool.

As shown below, the user will enter a file name and click the *Add* button on this page. The application will then provide a button for detailed information. The user will click the *Describe* button and then browse to select a file on their computer or network to submit.

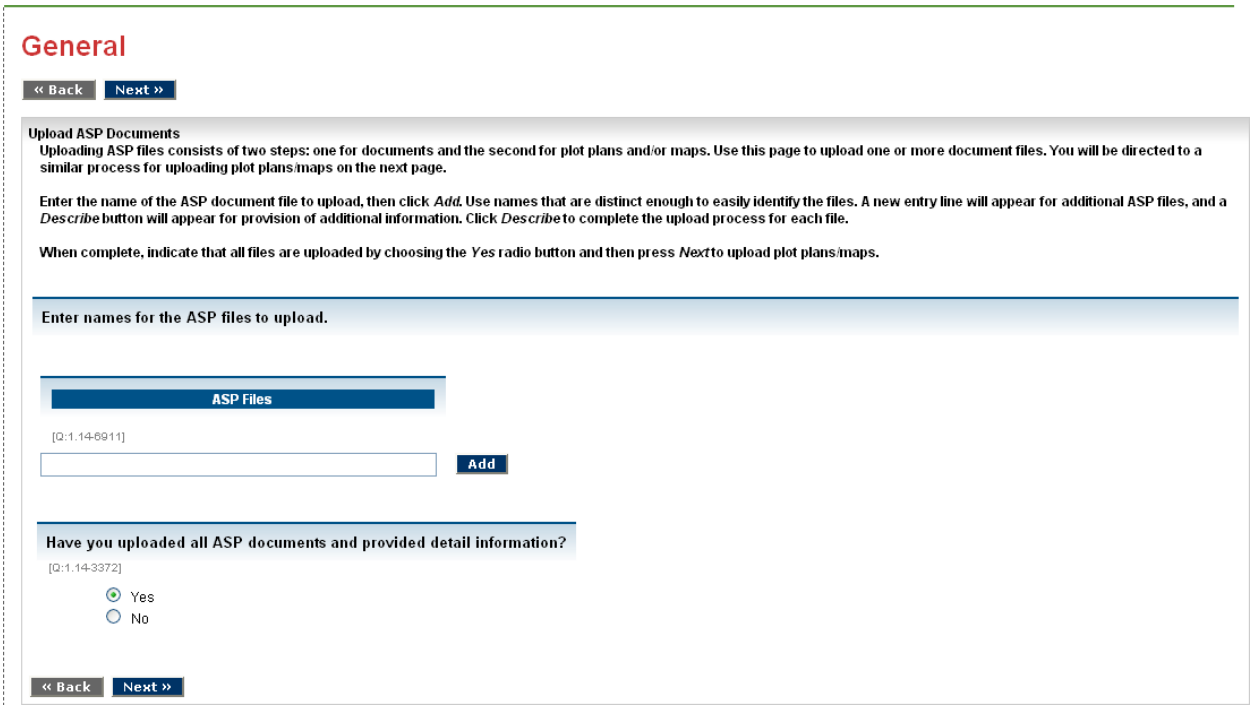

Figure 2-5 Upload ASP Documents Screen

Upload ASP. [Q:1.14-6911] List the name of the ASP file to upload and click the *Add* button. The file names should be distinct enough to identify the files during the next step. Once a file name is added, another *Add* button will be displayed for the user to add all necessary files. This can be continued until all ASP files that the user wants to include with the submission have been named.

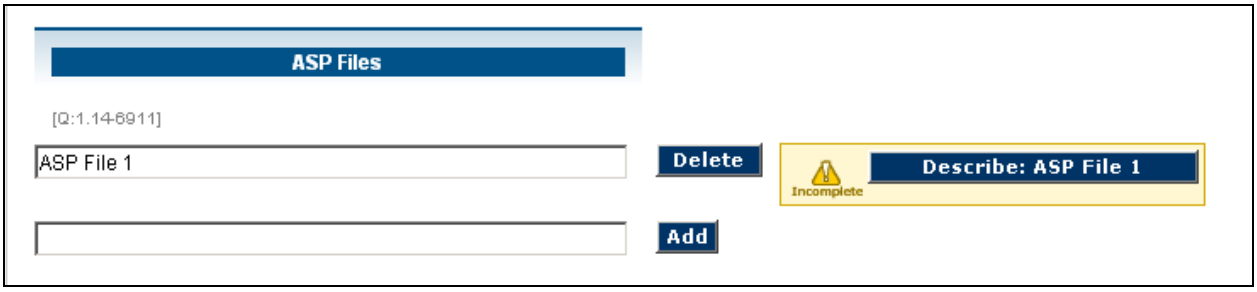

Figure 2-6 Provide Detail ASP Information

Next to each file name, the *Describe* button appears. For each file, click this button and complete the following information.

Click on the *Browse* button to locate the ASP file on your computer or network. When the file is located, click the *Add* button to upload the file.
Enter a description of the uploaded file.[Q: 1.15-6912] Click *Next* when complete.

Confirmation of ASP Upload. [Q:1.14-3372] Have all the ASP files been uploaded? Select *Yes* to continue with the ASP upload process. Select *No* if additional information needs to be selected and included in the transmittal to DHS.

2.2.3 Plot Plans/Maps

The next screen enables the user to provide the names of the plot plan/map files that were uploaded. Ensure that the locations of assets that were analyzed in the 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.

Plot Plan/Map Names. [Q:1.3-3354] Enter names for the plot plan/maps of the facility site. For each of the plot plans/facility maps uploaded the names of the maps are entered in this section for identification at DHS. As shown, the user will enter a file name and click the *Add* button on this page. The application will then provide a button for detailed information. The user will click the *Provide Detail* button and then browse to select a file on their computer or network to submit. Once a name is added, another file name can be added, this can be continued until all file names of the uploaded plot plans/facility maps have been added.

2.2.4 Map Image Details

Browse to locate Map files for uploading. Click on the *Browse* button to locate the Map file on your computer or network. For each map image, the following detail information needs to be provided.

Image width (miles) [Q:1.31-3356]
Image height (miles) [Q:1.31-3357]

Click *Next* to complete the survey.

Confirmation of SVA Upload. [Q:1.3-3355] Have you completed uploads of maps? Select *Yes* to confirm all maps of the facility have been uploaded as part of the ASP.

2.2.5 ASP Submission

A Tier 4 facility that answers the questions and uploads an ASP in lieu of a SVA as instructed in Section 2.2, has completed the use of this CSAT SVA tool. This information will be uploaded to DHS, and the facility will be contacted with the results of the review of the ASP and the next steps, if any, under CFATS.

The first screen that the user will see after completing the ASP upload is the *ASP Submission* screen, which states:

> ***Thank you for submitting an ASP in lieu of the CSAT SVA for consideration by DHS. DHS will review your ASP submission and subsequently inform you of its acceptance or rejection.***

User clicks *Next* after reading.

2.2.6 Completion

Instructions on final validation, including the fact that the user submitted an ASP, and final submission are detailed in Section 7.

3.0 Facility Security Issues

The first step of the CSAT SVA process is to define the security issues and Chemicals of Interest (COI) for the facility. The information entered into this section will enable the user to define assets (in the Asset Characterization section), and is the basis for identifying the applicable attack scenarios (in the Vulnerability Analysis section). To complete this section, the user should refer to the DHS initial notification letter that identifies the facility's security issue(s) and the related COI.

If the SVA has been pre-populated, the Summary of Facility Security Issues (see Figure 3-2) will be displayed.

3.1 Reporting Facility Security Issues

In 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. Only the identified security issues documented by DHS in this letter must be entered into the CSAT SVA. For some facilities this information may be pre-populated. 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 this section of CSAT SVA is selected, either from the navigation bar or following the completion of the information under **General**, the user will be asked a series of seven questions. The specifics are detailed below and consist of the security issues. These questions require the user to identify which security issues were reported by DHS in the initial notification letter.

These questions are illustrated on the following page.

Answer *Yes* or *No* to the following questions. Then click *Next*.

Release-Toxic Chemicals of Interest (COI). [Q:2.0-971] Does the DHS initial notification letter indicate that the facility should address security issues related to release-toxic COI?

Release-Flammable Chemicals of Interest (COI). [Q:2.0-3131] Does the DHS initial notification letter indicate that the facility should address security issues related to release-flammable COI?

Release-Explosive Chemical of Interest (COI). [Q:2.0-3132] Does the DHS initial notification letter indicate that the facility should address security issues related to release-explosive COI?

Theft/Diversion-Explosive/Improvised Explosive Device Precursor Chemicals of Interest (COI). [Q:2.0-3172] Does the DHS initial notification letter indicate that the facility should address security issues related to theft-EXP/IEDP COI?

Theft/Diversion-Weapons of Mass Effect Chemical of Interest (COI). [Q:2.0-3171] Does the DHS initial notification letter indicate that the facility should address security issues related to theft-WME COI?

Theft/Diversion-CW/CWP Chemicals of Interest (COI). [Q:2.0-3151] Does the DHS initial notification letter indicate that the facility should address security issues related to theft-CW/CWP COI?

Sabotage/Contamination Chemical of Interest. [Q:2.0-3173] Does the DHS initial notification letter indicate that the facility should address security issues related to sabotage/contamination COI?

3.2 Reporting Chemicals of Interest

Depending on the number of security issues reported in the previous section, up to seven additional screens will be displayed for the user to report the specific chemicals of interest (COI) related to those security issues and identified in the DHS initial notification letter. These are the chemicals (along with the security issues) that will be the focus of the CSAT SVA. For each security issue/chemical combination, the user must select the COI identified under each security issue in the DHS initial notification letter.

Release-Toxic Chemicals of Interest. [Q:2.1-1037] 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. The user must change the answer to *Yes* for each chemical listed in the letter under the security issue **Release of Toxic Chemicals**.

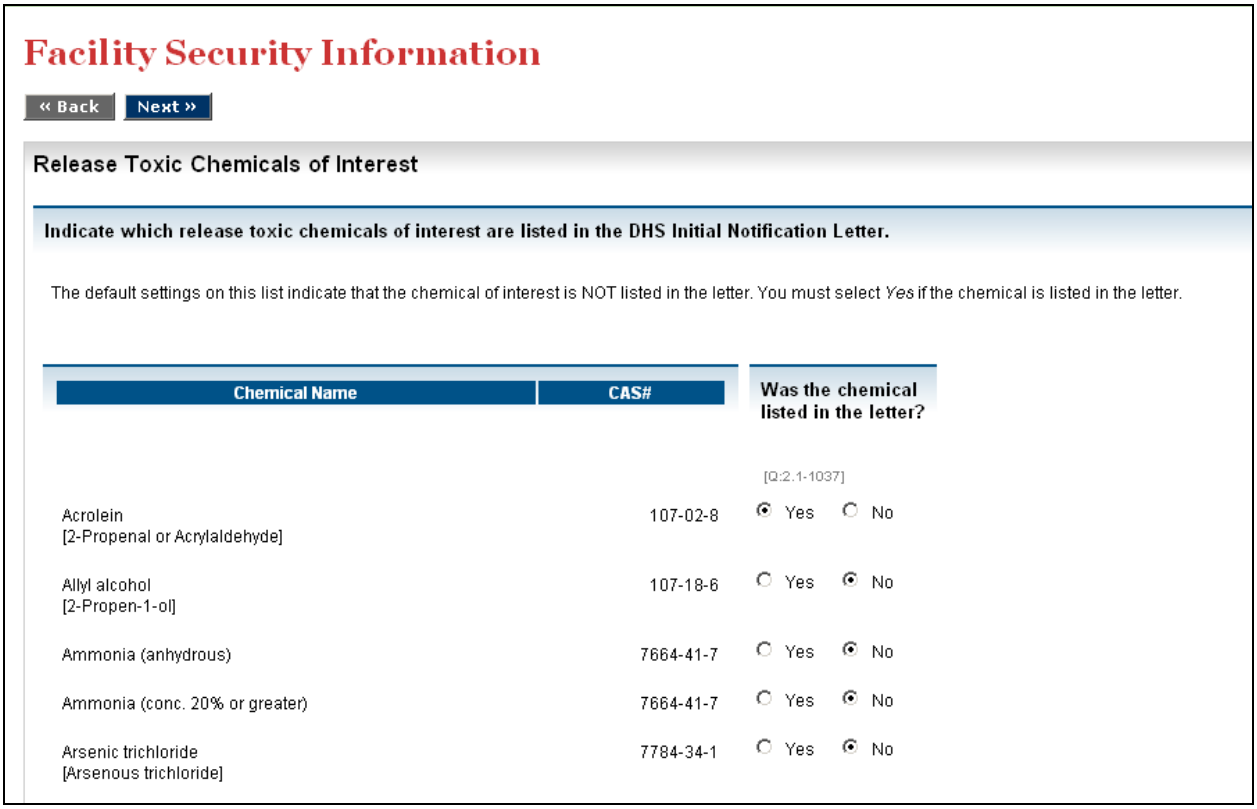

Figure 3-1 Toxic COI Screen

Release-Flammable Chemicals of Interest. [Q:2.2-1038] 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. The user must change the answer to *Yes* for each chemical listed in the letter under the security issue **Release-Flammable Chemicals.**

Release-Explosive Chemicals of Interest [Q:2.3-1039] Was the release-explosive chemical listed in the 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 **Release-Explosive Chemicals**.

Theft/Diversion-Explosive/IED Precursor Chemicals of Interest. [Q:2.6-1043] Was the chemical 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-Explosive/IED Precursor Chemicals**.

Theft/Diversion-WME Chemicals of Interest. [Q:2.5-1042] Was the chemical listed in the 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-WME Chemicals.**

Theft/Diversion-CW/CWP Chemicals of Interest. [Q:2.4-1041] Was the chemical listed in the 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**.

Sabotage/Contamination Chemical of Interest. [Q:2.7-1671] Was the chemical listed in the 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.**

3.3 Summary of Facility Security Issues

After the user has indicated all of the COI included in the DHS initial notification letter, a summary page is shown, highlighting the COI that the user indicated were in the letter. The information on this page should match the COI and security issue(s) identified in the DHS initial notification letter. It is critical that all COI and security issues are entered before moving on to the next steps of the CSAT SVA, which are based on that information.

A screen shot illustrating this summary information is on the following page.

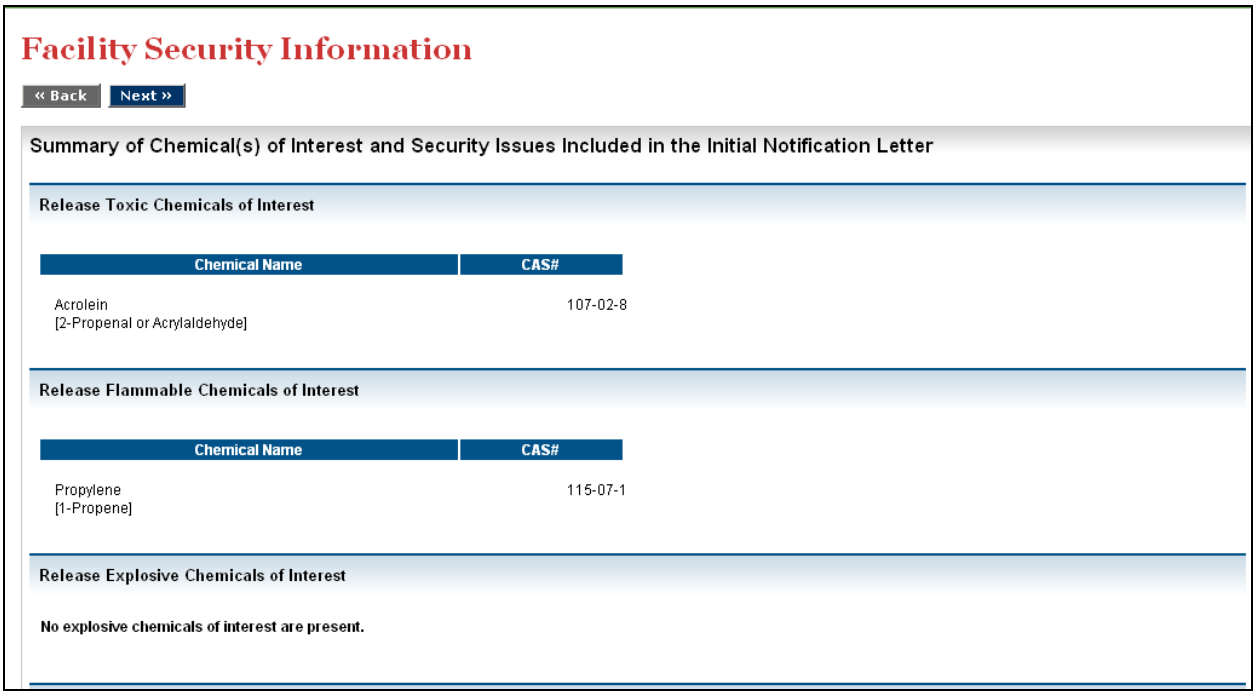

Figure 3-2 Summary of Facility Security Issues Selected

Once the summary is reviewed, the user must answer *Yes* or *No* to the following question.

Confirmation of security issues and COI. [Q:2.98-3411] Have all of the security issues and COI from the DHS initial notification letter been entered?

If the user answers *No*, then the user is directed back to the beginning of the **Facility Security Issues** section of the CSAT SVA. If *Yes*, then the user continues with Facility Characteristics.

3.4 Facility Characteristics

For facilities that have a Release Toxic COI

Facility Topography [Q:2.92-5911] What is the surrounding topography of the facility? Select the option, *Urban* or *Rural* that best defines the area surrounding the facility. The entry here should match the corresponding entry in the CSAT Top-Screen. As in the Top-Screen, if a facility is covered by EPA's Risk Management Plan (RMP) rule (40 CFR Part 68), the selection of urban or rural 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 still unsure, select *Rural*.

Is the facility located on a navigable waterway? [Q:2.92-3313] Facilities should answer *Yes* to this question if a waterway along any portion of the facility perimeter can accommodate small to large watercraft. This includes vessels ranging from small pleasure craft, barges, and deep draft vessels. Facilities responding *No* will not evaluate a Maritime attack mode as part of the vulnerability analysis because it is not applicable for this facility.

3.5 Facility Security Information

On the following Facility Security Issues screens, the user enters information about equipment, systems, inventory, and personnel controls.

3.5.1 Security Equipment at the Facility

The facility has security equipment. [Q:2.93-12211] If the facility has any security equipment that helps reduce the vulnerability of COI that the DHS Initial Notification letter noted select the *Yes* radio button and answer the additional questions on the screen. If the facility does not have any security equipment to help reduce the vulnerability of COI that the DHS Initial Notification letter noted, select the *No* radio button and click *Next*.

List any security equipment at the facility that might help reduce the vulnerability of COI that the DHS initial notification letter noted as contributing to a high level of security risk. List only security equipment that applies across the facility, as opposed to equipment related to a specific COI or asset.

Possible examples of security equipment include[2]:

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

Possible examples of information related to security equipment:

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

[2] Note that these and other examples provided in this document are merely illustrative and are neither exclusive nor exhaustive. In addition, such examples are intended simply to assist facilities in completing the CSAT SVA and do not imply that any of the examples are present at any given facility.

Equipment	Location	Support Systems Required
Perimeter fence line at 7ft 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

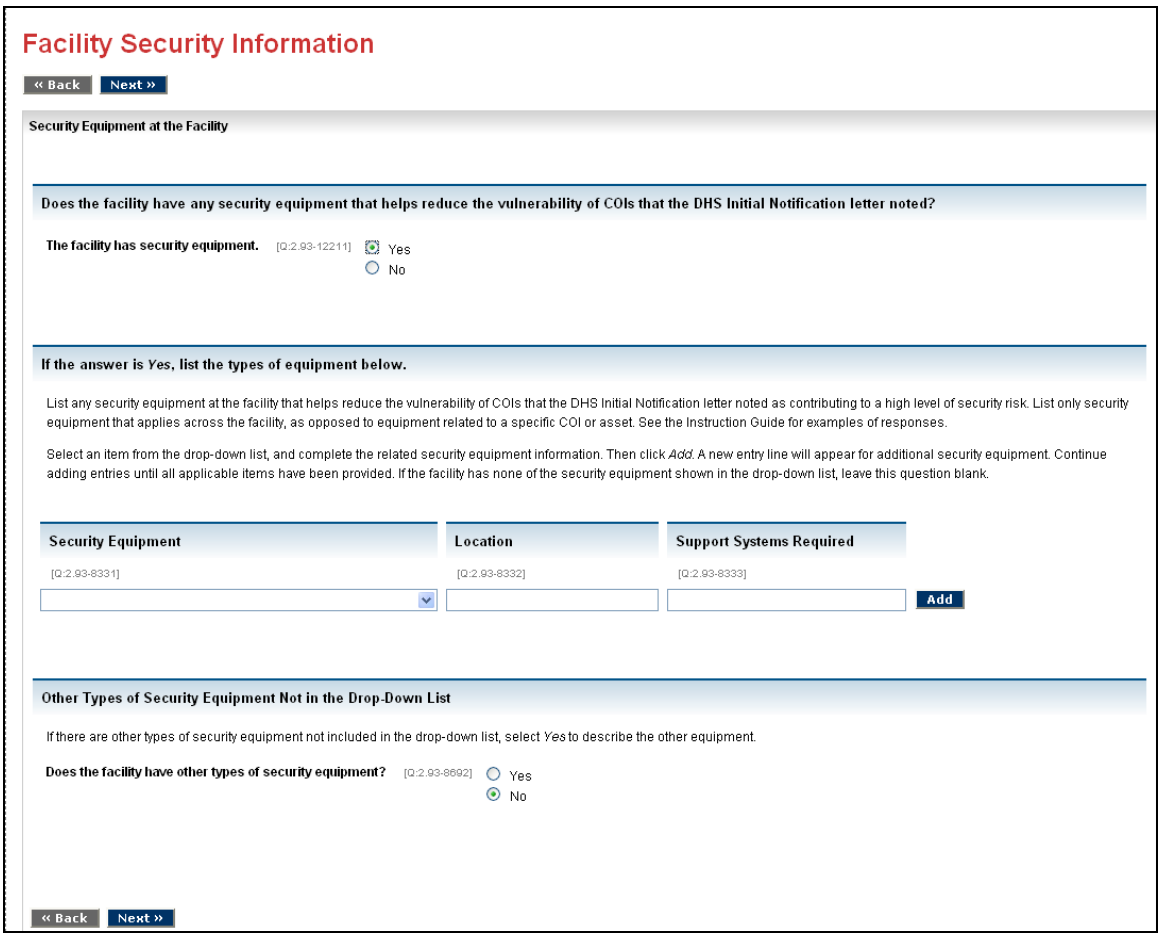

Figure 3-3 Security Equipment Screen

Security Equipment [Q: 2.93-8331] Use the drop-down list to select the name of the security equipment.
Equipment Location [Q: 2.93-8332] Enter the location of the equipment.
Support System [Q: 2.93-8333] Enter any support systems required to run the equipment.

Select an item from the drop-down list, and complete the related security equipment information. Then click *Add*. A new entry line will appear for additional security equipment. Continue adding entries until all applicable items have been provided. If the facility has none of the security equipment shown in the drop-down list, leave this question blank. If the security equipment desired is not included in the drop-down list, answer *Yes* to the question below regarding other security equipment.

Other Security Equipment. [Q:2.93-8692] If there are other types of security equipment at the facility not included in the drop-down box, use the radio button to select *Yes* to describe the other equipment.

3.5.2 Additional Security Equipment

Are there other types of security equipment at the facility that reduce the vulnerability of COI and that are not previously listed? Only list security equipment that applies across the facility, as opposed to equipment related to a specific COI or asset.

Security Equipment Description [Q:2.931-8693] Describe additional security equipment.
Location. [Q:2.931-8694] Enter the location of the equipment.
Support Systems Required. [Q:2.931-8695] List any support systems required.

Enter the description and complete the related security equipment information. Then click *Add*. A new entry line will appear for additional security equipment. Continue adding entries until all applicable items have been provided.

3.5.3 Utility Systems and Infrastructure Support

The facility has utility systems or infrastructure support. [Q:2.94-12231] If the facility has any utility systems or infrastructure support required for the security equipment, select the *Yes* radio button 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 the *No* radio button and click *Next*.

List utility systems or other infrastructure support required by the security equipment and specify where on the facility the system or equipment is located.

Possible examples of utility systems/infrastructure include:

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

Possible example of information related to utility system or infrastructure:

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.

System/Infrastructure [Q: 2.94-8351] Use the drop-down list to select the name of the system/ infrastructure.
System Location [Q: 2.94-8352] Enter the location of the system or infrastructure.

Select an item from the drop-down list and complete the related system/infrastructure information. Then click *Add*. A new entry line will appear for additional entries. Continue adding entries until all applicable items have been provided. If the facility has none of the system/infrastructure shown in the drop-down list, leave this question blank. If the system/infrastructure desired is not included in the drop-down list, answer *Yes* to the question below regarding *other utility systems*.

Other Utility Systems. [Q:2.94-8696] If there are other types of utility systems at the facility that are not included in the drop-down list, use the radio button to select *Yes* to describe the other equipment.

3.5.4 Additional Utility Systems

List additional utility systems or other infrastructure support required for the security equipment and the location of the systems or equipment.

System/Infrastructure [Q:2.941-8698] Enter the description of the system or infrastructure.
System Location [Q:2.941-8699] Enter the location of the system or infrastructure.

Enter the description and location. Then click *Add*. A new entry line will appear for additional System/Infrastructure. Continue adding entries until all applicable items have been provided.

3.5.5 Inventory Control Measures

If the facility's DHS initial notification letter included any theft/diversion-COI, list any inventory control measures at your facility that would be useful in reducing vulnerability of theft/diversion-COI.

The facility has inventory control measures. [Q:2.95-12235] If the facility has any inventory control measures that would help reduce vulnerability to theft/diversion select the *Yes* radio button 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 the *No* radio button and click *Next*.

Possible examples of inventory control measures include:

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

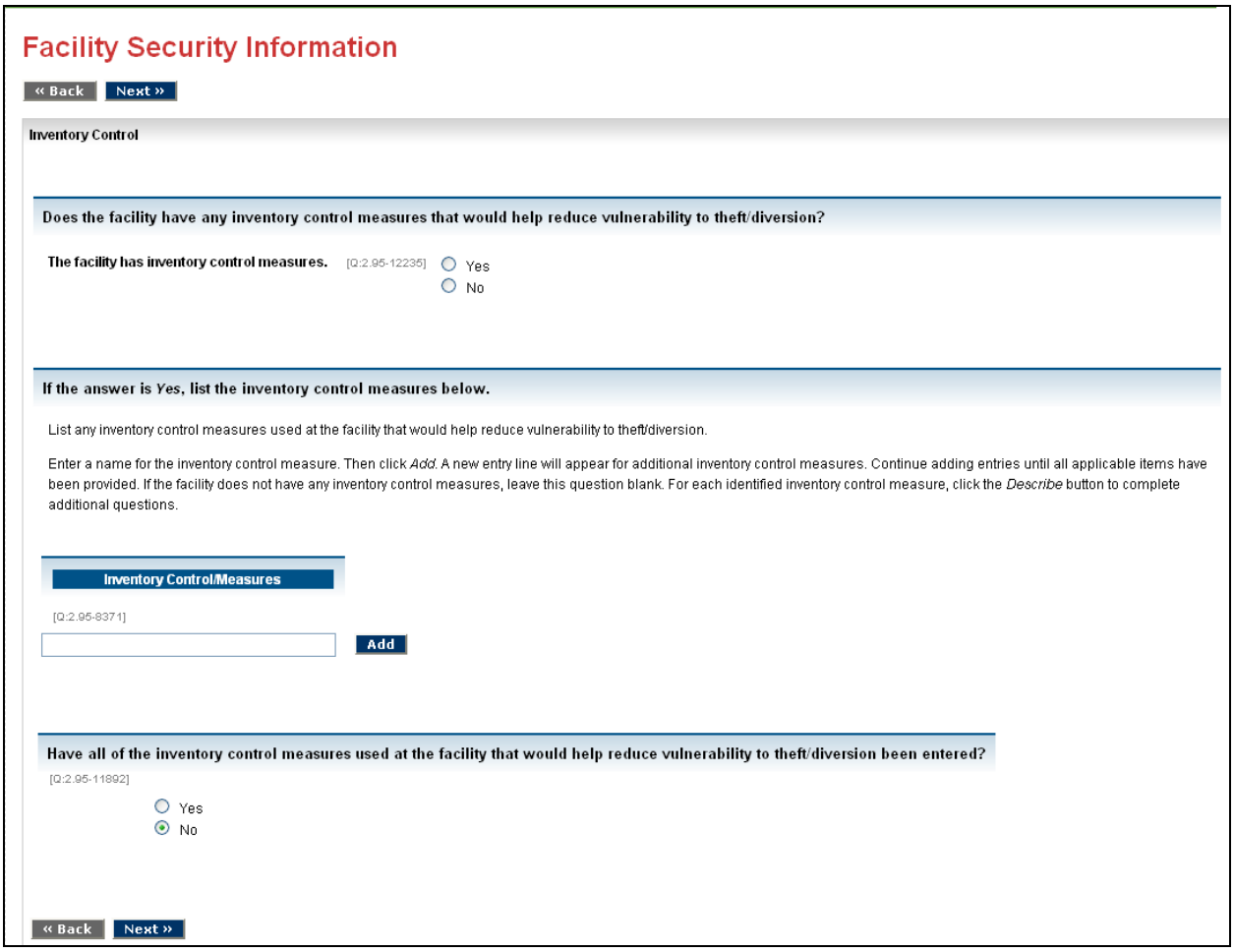

Figure 3-4 Inventory Control Screen

Inventory Control [Q: 2.95-8371] Enter the inventory control measure.

Enter a name for the inventory control measure. Then click *Add*. A new entry line will appear for additional inventory control measure. Continue adding entries until all applicable items have been provided. If the facility does not have any inventory control measures, leave this question blank. For each identified inventory control measure, click the *Describe* button to complete additional questions.

Facility Security Information

« Back | Next »

Inventory Control - Details

Logging of all inventory transactions in the R&D Lab sensitive chemical storage area

Please note if the inventory control system is automated or manual, the frequency with which it is applied, the location of the system, the inventory procedure, and whether procedure applies to the COI. See the Instruction Guide for examples of responses.

Is the inventory procedure automated?
[Q:2.951-8711]

- ○ Yes
- ◉ No

Frequency Applied
[Q:2.951-8372]

Daily

Location
[Q:2.951-8373]

R&D Lab sensitive chemical storage area

Inventory Procedure
[Q:2.951-10451]

- ☐ Continuous electronic inventory accounting for all COI
- ☐ Periodic electronic inventory accounting for all COI
- ☐ Periodic, manual inventory accounting for all COI
- ☐ Recordkeeping procedures that track customer orders
- ☐ Recordkeeping procedures that identify suspicious orders and inquiries
- ☐ Recordkeeping procedures that report inventory discrepancies to regulatory and/or law enforcement agencies
- ☐ Restricted access to customer ordering system
- ☐ Restricted access to customer information
- ☐ Training for customer sales representatives on handling suspicious orders or inquiries
- ☐ Background checks for customer sales representatives
- ☑ Inventory reconciliation procedures
- ☑ Inventory reconciliation procedures that identify, investigate, and resolve shortages
- ☐ Procedures for reporting shortages to regulatory and/or law enforcement agencies
- ☑ Product segregation procedures
- ☑ Restricted access to segregated products

Theft/Diversion Chemical Weapon/Chemical Weapon Precursor (CW/CWP) Chemicals of Interest

Chemical Name	CAS#	Does procedure apply to COI? [Q:2.951-8573]
Arsenic trichloride [Arsenous trichloride]	7784-34-1	◉ Yes ○ No

« Back | Next »

Figure 3-5 Inventory Control Details Screen

Automated Measure.[Q:2.951-8711] Is the inventory procedure automated?
Frequency Applied [Q: 2.951-8372] Use the drop-down list to indicate the frequency with which the measure is applied.
Control Location [Q: 2.951-8373] Enter the location of the inventory control measure.
Inventory Control Measure [Q: 2.951-10451] Use the check boxes to indicate which inventory control measures are used. Check all that apply.
Chemicals Covered by the Measure. [Q:2.951-8511], [Q:2.951-8571], [Q:2.951-8573] Identify any COI that are covered by the Inventory Control measure.

Click *Next* to return to the Inventory Control Measure Screen.

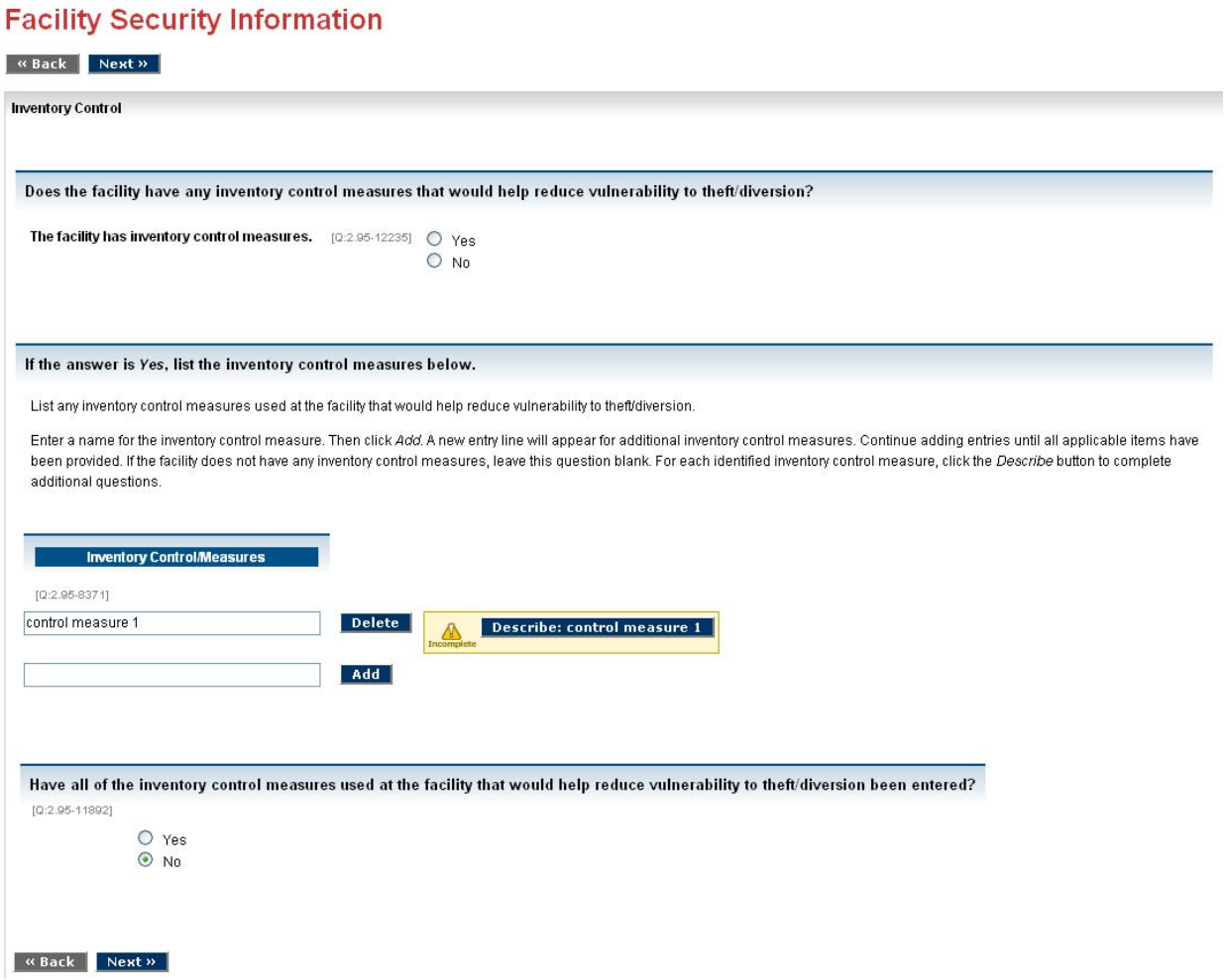

Figure 3-6 Incomplete Inventory Control Screen

When the user has completed the description screens, the user will be asked if the description is complete (a check box). When the user indicates that the questions are complete, they will return to the list of inventory control measures. If the user marked the item complete and all required questions were answered for that item, the item will be displayed with a green check mark icon. If the user does not check the box to indicate that the questions are complete, or if any required questions were not answered, the item will be displayed with a yellow warning icon as a reminder that the item is incomplete. Click *Next*.

3.5.6 Personnel Access Control Measure

The facility has personnel access control measures. [Q:2.96-12232] If the facility has any personnel access control measures that would help reduce vulnerability to an attack select the *Yes* radio button 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 the *No* radio button and click *Next*.

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

Possible examples of personnel access control systems 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 assets.

Possible examples of information on personnel access control systems include:

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

Access Control Measure [Q: 2.96-8431] Use the drop-down list to select the personnel access control measure. The drop-down list options:

- 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

Control Measure Q:2.96-8712] Indicate whether the control measure is automated or not.
Frequency Applied [Q: 2.96-8432] Use the drop-down list to indicate the frequency with which the measure is applied.
Location [Q: 2.96-8433] Enter the location of the control measure.
Personnel Covered [Q: 2.96-8434] Enter the personnel that are covered by this measure.

Select an item from the drop-down list and complete the personnel access control measure information. Then click *Add*. A new entry line will appear for additional personnel access control measure information. Continue adding entries until all applicable items have been provided. If the facility has none of the personnel access control measures shown in the drop-down list, leave this question blank. If the personnel access control desired is not included in the drop-down list, answer *Yes* to the question below regarding other personnel access controls.

Other Personnel Access Control Measures. [Q:2.96-8713] If there are other types of personnel access control measures at the facility that are not included in the drop-down list, use the radio button to select *Yes* to describe these other measures.

3.5.7 Additional Personnel Access Controls

List additional personnel access controls.

Personnel Access Control Description [Q:2.961-8714] Enter a description of the access control measure.
Control Measure [Q: 2.961-8715] Indicate whether the control measure is automated or manual.
Frequency Applied [Q: 2.961-8716] Use the drop-down list to indicate the frequency with which the measure is applied.
Location [Q: 2.961-8717] Enter the location of the control measure.
Personnel Covered [Q: 2.961-8718] Enter the personnel that are covered by this control measure.

Enter the description and information. Then click *Add*. A new entry line will appear for additional personnel access control measures. Continue adding entries until all applicable items have been provided.

3.5.8 Shipping and Receiving Control Measures

If the facility's DHS initial notification letter noted any theft/diversion or sabotage/contamination COI, list any shipping and receiving measures in place at the facility that would be considered useful in reducing vulnerability to an attack.

The facility has shipping and receiving control measures. [Q:2.97-12236] If the facility has any shipping and receiving measures in place at the facility that would be considered useful in reducing vulnerability to an attack select the *Yes* radio button and answer the additional questions on the screen. If the facility does not have any shipping and receiving measures in place at the facility that would be considered useful in reducing vulnerability to an attack select the *No* radio button and click *Next*.

Possible examples of information on shipping and receiving measures include:

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

Control Measures [Q:2.97-8611] Enter the shipping/receiving control measures.

Enter a name for the shipping and receiving measure. Then click *Add*. A new entry line will appear for additional shipping and receiving measures. Continue adding entries until all applicable items have been provided. If the facility does not have any shipping and receiving measures, leave this question blank. For each identified shipping and receiving measure click the *Describe* button to complete additional questions.

For each Control Measure:

Control Measure [Q:2.971-8719] Is the control measure automated or manual?
Frequency Applied [Q:2.971-8612] Use the drop-down list to choose the frequency with which the measure is applied.
Control Location [Q:2.971-8613] Enter the location of the control measure.
Control Measures [Q:2.971-10012] Use the check boxes to indicate the control measures in place. Check all that apply.
Chemicals Covered by Measure. [Q:2.971-8659], [Q:2.971-8665], [Q:2.971-8666], [Q:2.971-8671] Identify any COI that are covered by the control measure.

When the user has completed the description screens, the user will be asked if the description is complete (a check box). When the user indicates that the questions are complete, they will return to the list of shipping control measures. If the user marked the item complete and all required questions were answered for that item, the item will be displayed with a green check mark icon. If the user does not check the box to indicate that the questions are complete, or if any required questions were not answered, the item will be displayed with a yellow warning icon as a reminder that the item is incomplete. Click *Next* to return to the Shipping/Receiving Control Measure Screen.

3.5.9 Post-release Measures and Equipment

The facility has post-release measures. [Q:2.98-12233] If the facility has any post-release measures or equipment that would be considered useful in reducing the consequence of a toxic release select the *Yes* radio button and answer the additional questions on the screen. If the facility does not have any post-release measures or equipment that would be considered useful in reducing the consequence of a toxic release select the *No* radio button and click *Next*.

List any post-release measures 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 mitigation systems include:

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

Possible examples of information for mitigation systems include:

Equipment/Application	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

Post-release Equipment/Application [Q:2.98-8451] Use the drop-down list to select any post-release measures or equipment that would be useful in reducing the consequence of a release-toxic COI release.
Location. [Q:2.98-8452]. Enter the location of the equipment.
Support Systems Required. [Q:2.98-8453] List any support systems required.

Select an item from the drop-down list, and complete the post-release measures or equipment information. Then click *Add*. A new entry line will appear for additional post-release measures or equipment. Continue adding entries until all applicable items have been provided. If the facility has none of the post-release measures or equipment shown in the drop-down list, leave this question blank. If the facility has post-release measures or equipment not listed in the drop-down list, answer *Yes* to the question below regarding *other post-release measures* to describe it.

Other Post-release measures. [Q:2.98-8720] If there are other types of post-release measures at the facility use the radio button to select *Yes* to describe the equipment.

3.5.10 Additional Post-release Measures

List any additional post-release measures or equipment that would be useful in reducing the consequence of a release-toxic COI release.

Post-release Equipment/Application [Q:2.981-8721] Describe any post-release measures or equipment that would be useful in reducing the consequence of a release-toxic COI release.
Location. [Q:2.981-8722]. Enter the location of the equipment.
Support Systems Required. [Q:2.981-8723] List any support systems required.

Enter the name of the post-release measures or equipment, and complete the information. Then click *Add*. A new entry line will appear for additional post-release measures or equipment. Continue adding entries until all applicable items have been provided.

Click *Next* when all post-release measures or equipment have been added.

3.5.11 Site Vulnerability Factors

The facility has site factors that increase vulnerability. [Q:2.99-12234] If the facility has any features, offsite terrain or infrastructure items that potentially increase the facility's vulnerability to attack select the *Yes* radio button 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 the *No* radio button and click *Next*.

List any facility features, offsite terrain or infrastructure items that potentially increase the facility's vulnerability to attack.

Possible examples of such features include:

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

Possible examples of such features include:

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 though 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

Site Vulnerability [Q:2.99-8454] Enter any facility features, offsite terrain, or infrastructure items that potentially increase the site's vulnerability to attack.
Comment [Q:2.99-8455] Add a comment/description.

Enter the site vulnerability, and complete the information. Then click *Add*. A new entry line will appear for additional site vulnerabilities. Continue adding entries until all applicable items have been provided. If the facility has no site vulnerabilities, leave this question blank.

Click *Next* when all site vulnerability factors have been added.

4.0 Asset Characterization

After completing the **Facility Security Issues** section, the **Asset Characterization** section will become available for selection on the navigation bar.

In this step, a facility identifies one or more assets associated with the COI and security issue(s) entered in the **Facility Security Issues** section.

For purposes of an SVA, assets characterized for analysis by a facility will vary by 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 location or other factors).

4.1 Identifying Assets

The 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). A primary COI is the COI for which the consequences of damage to that asset will be estimated. The CSAT SVA is set up so that each asset is associated with **one Primary COI**. Thus, an asset that is associated with more than one COI might need to be identified multiple times, listing each COI as Primary in turn.

For example:

The user has a building housing COI "x" and "y".
Asset 1 would be the building and list the Primary COI as "x".
Asset 2 would be the same building but list the Primary COI as "y".

The instructions below indicate the criteria for identifying assets based on the type of COI. Please refer to the DHS initial notification letter, or print a copy of the summary of facility security issues described in the previous section.

The specific instructions below 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 purposes of these instructions, any hardware, packaging, or other containers holding a COI is referred to as "equipment."

Assets Are Required for Each COI and Security Issue Combination

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: release and theft/diversion. In most cases, these assets would be distinct equipment items (e.g., a bulk storage tank and a portable container) but 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, as well as for theft/diversion.)

Asset Identification for Release COI

Identify one or more assets for each release COI (i.e., release-toxic, release-flammable, or release-explosive) included by DHS in the facility's DHS initial notification letter. Assets must be characterized for each release COI.

Identify assets for the release scenarios as follows:

1. Identify as an asset the equipment at the facility that contains the largest inventory of the specific COI being considered. 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 1 above and where the vulnerability of that asset to attack is expected to be greater than for the asset identified in 1 above (because of 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 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 1 above).

4. If an equipment item contains the largest inventory of two different COI identified in the Facility Security Section, it should be treated as two separate assets, one for each COI.

Asset Identification for Theft/Diversion COI

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.

Identify assets for theft/diversion scenarios that meet the following criteria:

1. Identify an asset for 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 for 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 1 above (because of portability, availability, ease of use by an adversary, and/or other factors).

Asset Identification for Sabotage/Contamination COI

Identify one or more assets for each sabotage/contamination COI identified by DHS 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.

Identify assets for sabotage/contamination scenarios as follows:

1. Identify an asset for the largest amount of the sabotage/contamination COI that the facility ships and that require a placard under Department of Transportation (DOT) hazardous materials regulations (Subpart F of 49 CFR Part 172).

2. Identify additional assets for smaller amounts of sabotage/contamination COI that the facility ships and that 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 1 above (because of availability, ease of use by an adversary, or other factors).

4.2 Characterize Assets

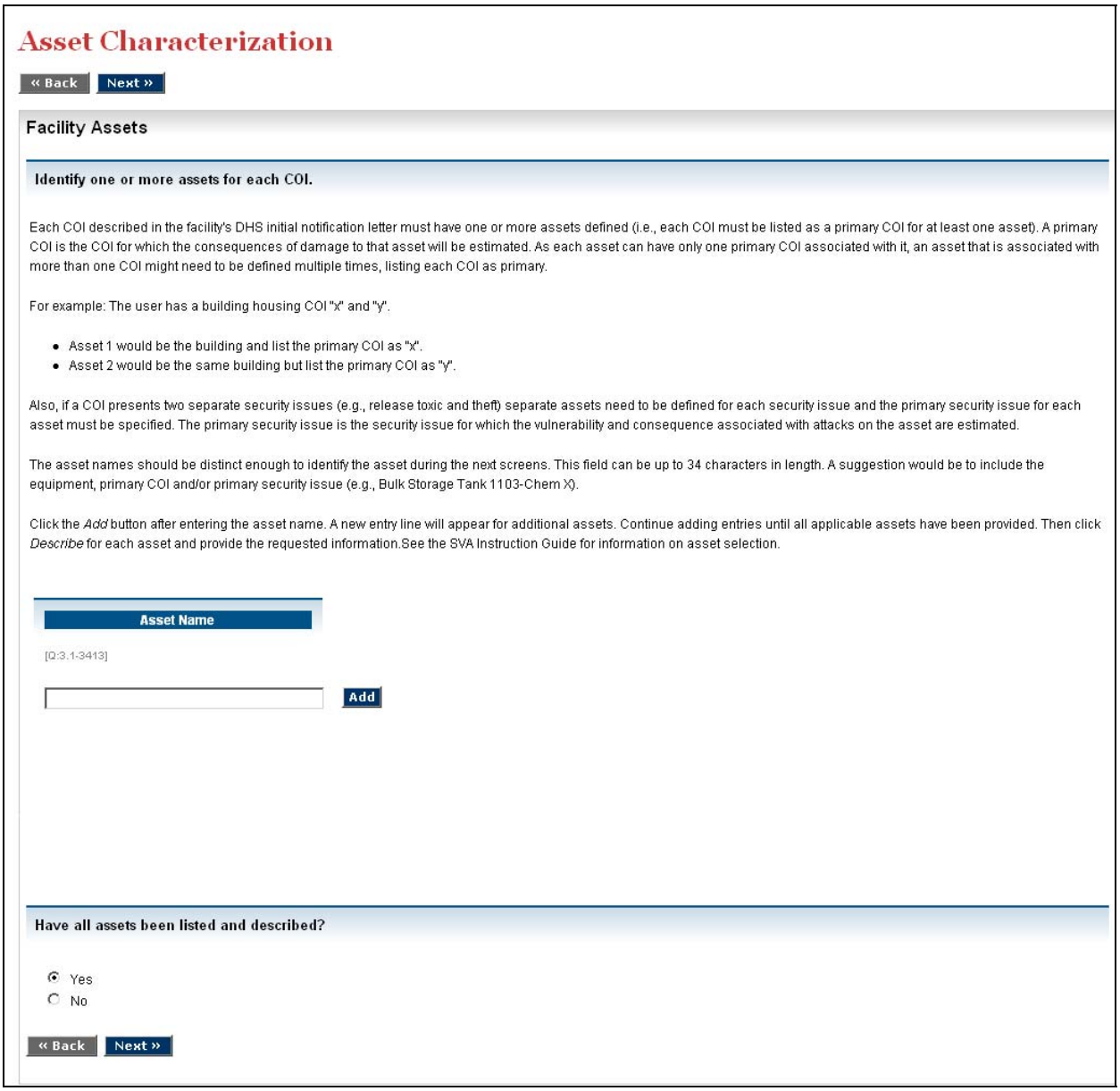

Figure 4-1 Asset Name Screen

Asset Name: [Q:3.1-3413] Enter the asset name in the space provided.

The Asset Name field can be up to 34 characters in length and contain a mix of alphanumeric data. The asset names should be distinct enough to identify the asset during the next screens, e.g., include the equipment, primary COI and/or the primary security issue as in the two examples below:

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

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

When the user has completed the asset description screens, the user will be asked if the description is complete (a check box). When the user indicates that the questions are complete, they will return to the list of assets. If the user marked the asset complete and all required questions were answered for that asset, the asset will be displayed with a green check mark icon. If the user does not check the box to indicate that the questions are complete, or if any required questions were not answered, the item will be displayed with a yellow warning icon as a reminder that the item is incomplete. The user can reference the green check mark or yellow warning icon as reminders of the status of each item.

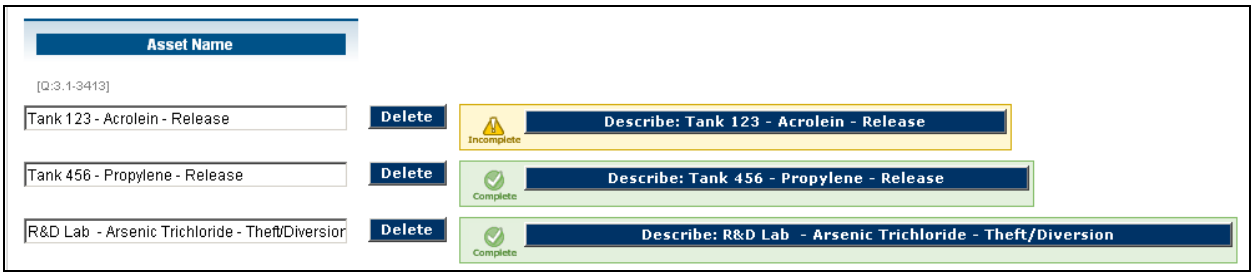

Figure 4-2 Describe Asset Screen

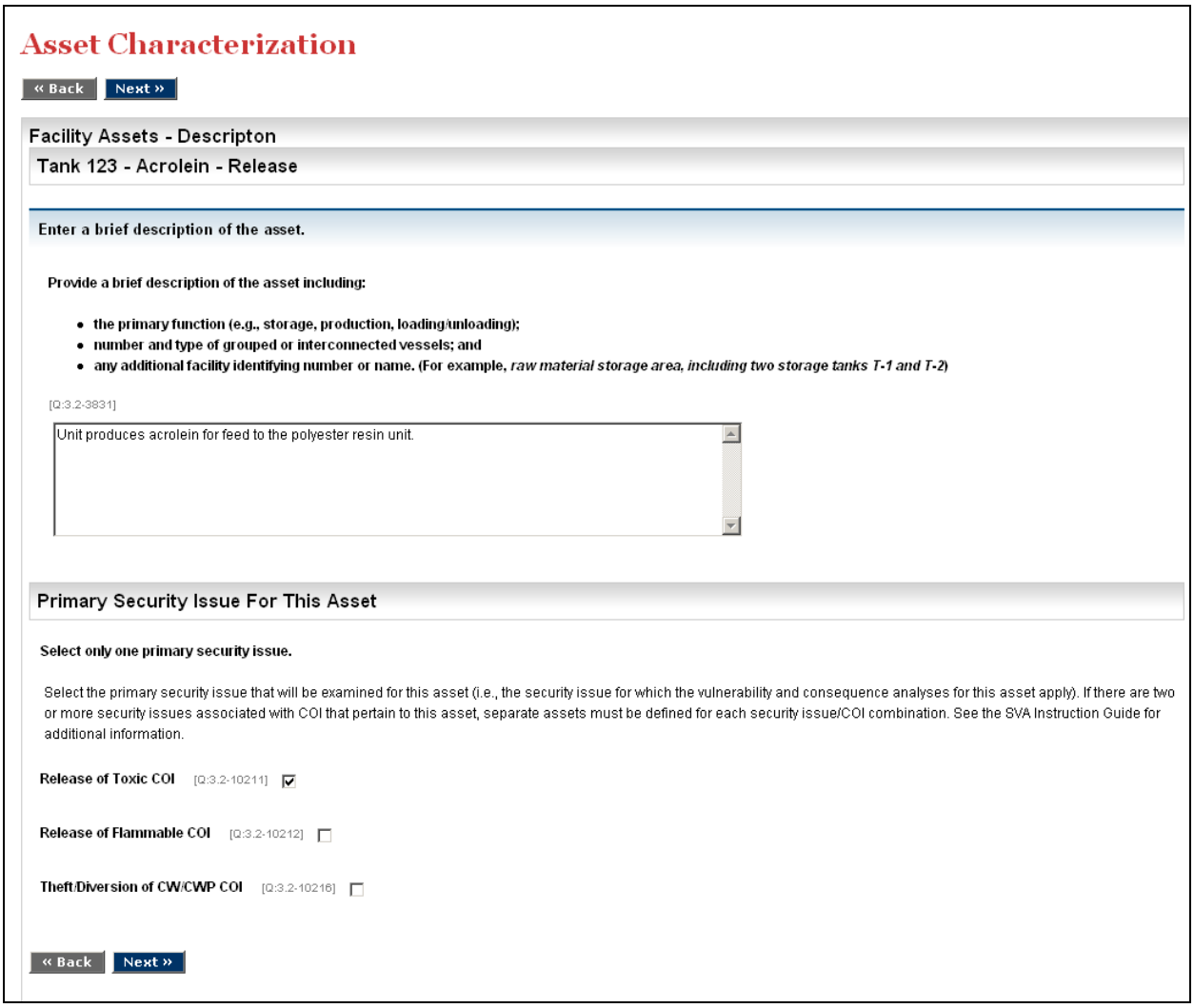

Figure 4-3 Asset Description Screen

Asset Description. [Q:3.31-3831] Enter a brief description of the asset in the space provided, including:

- The primary function (e.g., storage, production, loading/unloading);
- Number and type of grouped or interconnected vessels; and
- Any additional facility identifying number or name. (For example, raw material storage area, including two storage tanks T-1 and T-2)

Select the primary security issue for this asset. [Q:3.2-10211-10217] 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. Also, 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 box.

Click *Next* for the Facility Assets Detail Screen.

For Release Security Issues
Containment Type. [Q:3.31-12192] Is the containment type used for this asset? Use the radio buttons to select the items where the COI is located or contained within this asset. Select as many as apply.

4.2.1 COI Associated with Asset

Use the radio buttons to identify the chemicals at this asset.

Note: Only COI that were entered as part of **Facility Security Issues** will be available for selection.

All COI associated with this asset should be selected here, regardless of whether they will be defined as the Primary COI for this asset.

Select all Release-Toxic Chemicals of Interest associated with this asset.
[Q:3.31-3473] Any release-toxic COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select all Release-Flammable Chemicals of Interest associated with this asset.
[Q:3.31-3493] Any release-flammable COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select all Release-Explosive Chemicals of Interest associated with this asset. [Q:3.31-3500] Any release-explosive COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select all Theft/Diversion-Explosive/Improvised Explosive Device Precursor (EXP/IEDP) Chemicals of Interest associated with this asset. [Q:3.31-3520] Any theft/diversion-EXP/IEDP precursor COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select all Theft/Diversion-Weapons of Mass Effect (WME) Chemicals of Interest associated with this asset. [Q:3.31-3514] Any theft/diversion-WME COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select all Theft/Diversion-Chemical Weapon/Chemical Weapons Precursors (CW/CWP) Chemicals of Interest associated with this asset. [Q:3.31-3507] Any theft/diversion-CW/CWP COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select all Sabotage/Contamination Chemicals of Interest associated with this asset. [Q:3.31-3527] Any sabotage/contamination COI identified in the Facility Security Issues Section will be listed here, check any that are associated with this asset.

Select *Next* to continue entering detail information on the asset.

4.2.2 Detailed COI Information for Asset

For each COI that has been identified at the asset, the user will be asked a series of questions, including which chemical is the Primary COI. Only screens for the identified chemicals will be shown (i.e., 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), the chemical information will need to be entered more than once. (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).

When calculating the quantity of COI, use the same counting rules provided by CFATS for calculating the applicable STQs for chemicals of interest.

Release-Toxic COI:

If the user indicated that a release-toxic was the primary security issue, the user will be asked to identify the primary COI and then provide detail information about each chemical at the asset. See Figure 4-4 for an example of this screen.

If the user indicated that a release-toxic chemical was associated with the asset (but not the primary security issue), the user will be asked detailed information about each release-toxic chemical at the asset. See Figure 4-5 for an example of this screen.

If no release-toxic chemical is associated with this asset, the user will not see the release-toxic chemical screen.

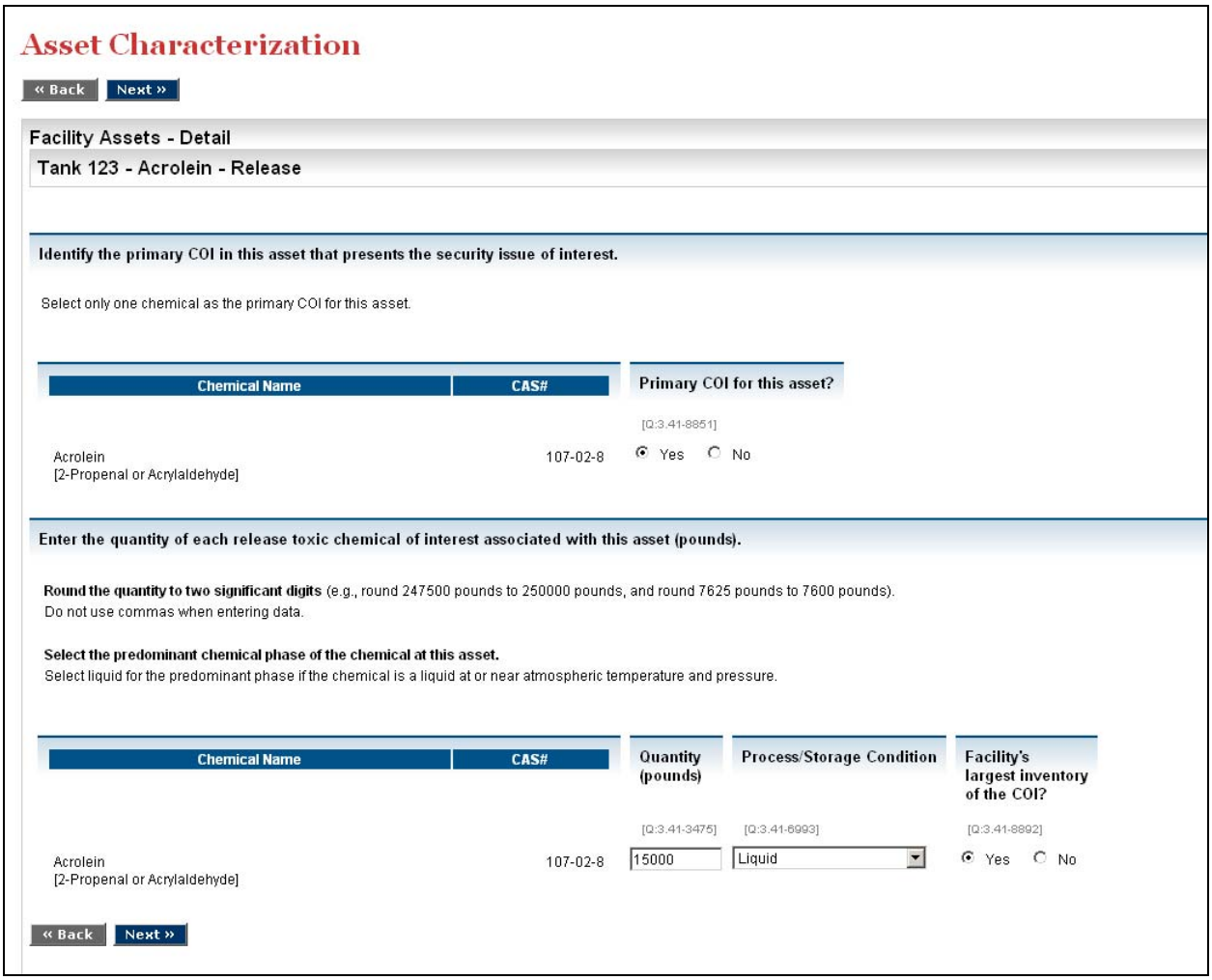

Figure 4-4 Asset Detail – Toxic Release Screen when the Asset's Primary Security Issue is Release-Toxic

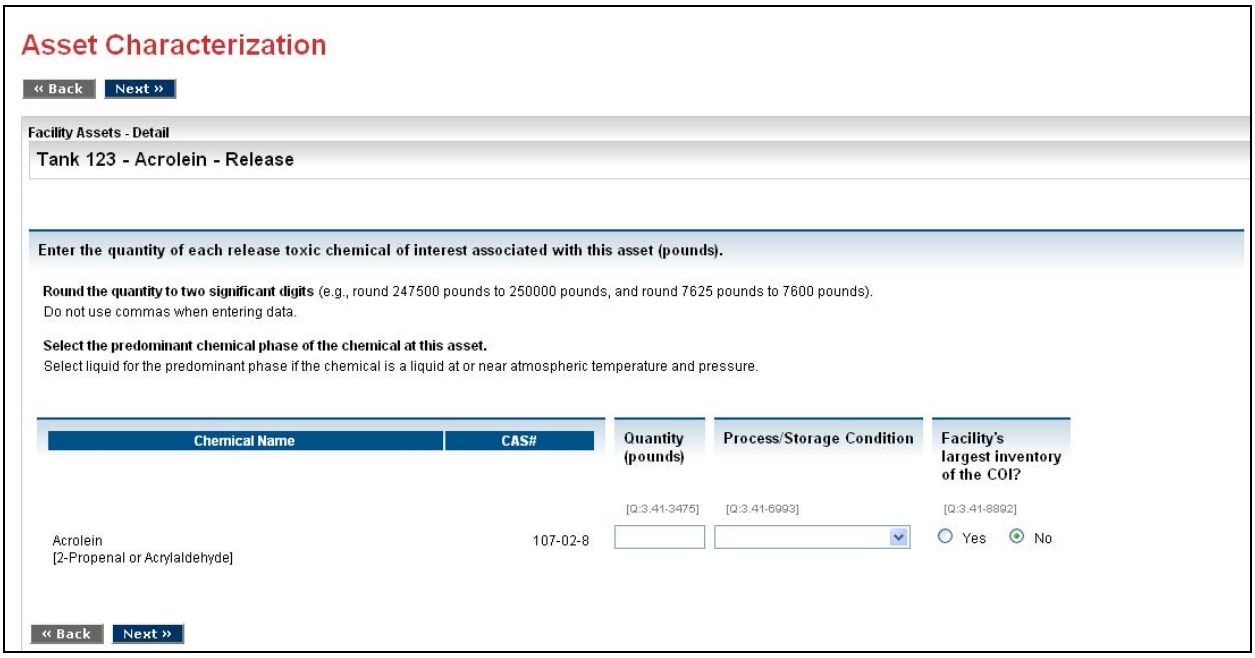

Figure 4-5 Asset Detail – Toxic Release Screen when the Asset's Primary Security Issue is NOT Release-Toxic

If the user indicated that this Asset's Primary Security Issue was a Release-Toxic COI
Indicate the Primary COI for this asset [Q:3.41-8851] 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 COI that should be the primary COI will need to be identified as multiple assets.

For each Release-Toxic COI at the asset
Quantity (pounds) [Q:3.41-3475] The user is required to enter the total quantity, in pounds, of each release- toxic chemical of interest 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.
Select the predominant chemical phase of the chemical at this asset. [Q:3.41-6993] Use the drop- down list to select the predominant chemical phase of the chemical at this asset. Select liquid for the predominant phase if the chemical is a liquid at or near atmospheric temperature and pressure.

Is the facility's largest inventory of the COI at this asset? [Q:3.41-8892] Answer *Yes* if the asset contains the largest inventory of the COI.

Select *Next* to continue.

For COI that were listed as predominantly liquids at this asset, the following questions will be asked:

Temperature (degree Fahrenheit) [Q:3.412-6995]
Process or storage pressure (psig) [Q:3.412-8893]
Liquid height (feet) [Q:3.412-8894] Enter the height of the liquid above the vessel bottom.

Is the liquid an aqueous solution? [Q:3.412-6996] If the answer to this question is *Yes*, the user will be directed to an additional question. **Percent Concentration by Weight** [Q:3.413-7011] Enter the initial percent concentration by weight of the toxic chemical in aqueous solution associated with this asset.

Select *Next* to continue.

For assets that have a Release-toxic as the primary security issue
Enter any mitigation 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 the user will be able to document whether these mitigation measures would be expected to survive an attack (see section 5.5.5).

Dike, berm, or other similar containment [Q:3.42-10471]
Leak detection system [Q:3.42-10472]
Fixed vapor suppression system [Q:3.42-10473]
Notification system for offsite evacuation or sheltering in place [Q:3.42-10474]
Other measures [Q:3.42-10475]

The user then clicks on the *Next* button to continue with the analysis. If any mitigation measures were checked, the user is directed to further detail mitigation screens. If no mitigation measures are in place, the user is directed to the next COI associated with the asset.

Dike, berm, or other similar containment
- **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 (e.g., fixed chemical detectors with alarm)
- **Description of system**[Q:3.421-9214]
- **Estimated time to detection for a toxic release (minutes)** [Q:3.421-9215]

Fixed vapor suppression system (e.g., foam or dry chemical cover, water spray system)
- **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 (e.g., phone dialing system, alarm system)
- **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
- **Description of other measures** [Q:3.421-9223]
- **Description of expected mitigation for a toxic release** [Q:3.421-9224]

Release-flammable COI:

If the user indicates that a release-flammable COI is the primary security issue, the user is asked to identify the primary COI and then provide detailed information about each chemical at the asset.

If the user indicates that a release-flammable COI is associated with the asset (but not the primary security issue), the user is asked detailed information about each release-flammable COI at the asset.

If no release-flammable COI is associated with this asset, the user will not see the release-flammable COI screen.

If the user indicates that this Asset's Primary Security Issue is a Release-Flammable COI
Indicate the Primary COI for this asset [Q:3.43-8854] 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.

For each Release-Flammable COI at the asset
Quantity (pounds) [Q:3.43-3496] The user is 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.
Is the facility's largest inventory of the COI at this asset? [Q:3.43-8971] Answer *Yes* if the asset contains the largest inventory of the COI.

Select *Next* to continue.

Release-explosive COI:

If the user indicates that a release-explosive COI is the primary security issue, the user is asked to identify the primary COI and then provide detail information about each chemical at the asset.

If the user indicates that a release-explosive COI is associated with the asset (but is not the primary security issue), the user is asked detailed information about each release-explosive COI at the asset.

If no release-explosive chemical is associated with this asset, the user will not see the release-explosive COI screen.

If the user indicates that this Asset's Primary Security Issue is a Explosive Release
Indicate the Primary COI for this asset? [Q:3.45-8856] 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 COI that should be the primary COI will need to be defined as multiple assets.

For each explosive COI at the asset
Quantity (pounds [Q:3.45-3503] The user is required to enter the total quantity, in pounds, of each explosive chemical of interest 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.

Is the facility's largest inventory of the COI at this asset? [Q:3.45-9005] Answer *Yes* if the asset contains the largest inventory of the COI.

Select *Next* to continue.

Theft/Diversion-Explosive/IEDPCOI:

If the user indicates that a Theft/Diversion of an Explosive/IEDP is the primary security issue, the user is asked to identify the primary chemical and then provide detailed information about each chemical at the asset.

If the user indicates that a Theft/Diversion Explosive/IED Precursor Chemical is associated with the asset (but not the primary security issue), the user is asked detailed information about each Explosive/IED Precursor COI at the asset.

If no Theft/Diversion Explosive/IED Precursor Chemical is associated with this asset, the user will not see the Explosive/IED Precursor COI screen.

If the user indicates that this Asset's Primary Security Issue is a Theft/Diversion Explosive/IED Precursor Chemical
Indicate the Primary COI for this asset? [Q:3.51-8858] 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.

For each Explosive COI at the asset
Is the facility's largest inventory of the COI at this asset? [Q:3.51-9167] Answer *Yes* if the asset contains the largest inventory of the COI.
Is the COI shipped offsite from this asset? [Q:3.51-5534] Answer *Yes* if the COI is shipped offsite from this asset.

Select *Next* to continue.

If the user indicated that this Assets Primary Security Issue was a Theft/Diversion Explosive/IED Precursor COI, the following questions will be asked about the primary COI.

COI concentration range [Q:3.52-9171] Use the drop-down list to select the concentration range of the COI in this packaging type (% by weight).
Packaging type description [Q:3.52-9172] Enter a brief description of the packaging type. Possible examples of transportation packaging include:

- Bottles
- Totes
- Carboys
- Boxes
- Drums
- Pressurized portable tanks and cylinders

Transportation packaging type [Q:3.52-9174] Use the drop-down list to select the transportation packaging type.

Total quantity of COI in this packaging type (lbs) [Q:3.52-9173] Enter the total quantity for this packaging type.

For chemicals that have multiple concentrations and/or transportation packaging types at this asset, enter the first instance and complete the related questions. Then click *Add*. A new entry line will appear for additional instances. Continue adding entries until all applicable instances have been provided. Select *Next* to continue.

Theft/Diversion-WME COI:

If the user indicates that a Theft/Diversion of a WME COI is the primary security issue, the user is asked to identify the primary COI and then provide detailed information about each chemical at the asset.

If the user indicated that a Theft/Diversion WME COI was associated with the asset (but not the primary security issue), the user is asked detailed information about each WME COI at the asset.

If no Theft/Diversion-WME COI are associated with this asset, the user will not see the WME COI screen.

If the user indicates that this Asset's Primary Security Issue is a Theft/Diversion WME COI
Indicate the Primary COI for this asset. [Q:3.49-8862] 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 COI that should be the primary COI will need to be defined as multiple assets.

For each WME COI at the asset
Is the facility's largest inventory of the COI at this asset? [Q:3.49-9094] Answer *Yes* if the asset contains the largest inventory of the COI.
Is the COI shipped offsite from this asset? [Q:3.49-5533] Answer *Yes* if the COI is shipped offsite from this asset.

Select *Next* to continue.

If the user indicates that this Asset's Primary Security Issue is a Theft/Diversion WME COI, the following questions will be asked about the primary COI.

COI concentration range [Q:3.5-9096] Use the drop-down list to select the concentration range of the COI in this packaging type (% by weight).
Packaging type description [Q:3.5-9097] Enter a brief description of the packaging type. Possible examples of transportation packaging include:

- Bottles
- Totes
- Carboys
- Boxes
- Drums
- Pressurized portable tanks and cylinders

Transportation packaging type [Q:3.5-9098] Use the drop-down list to select the transportation packaging type.

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

For chemicals that have multiple concentrations and/or transportation packaging types at this asset, enter the first instance and complete the related questions. Then click *Add*. A new entry line will appear for additional instances. Continue adding entries until all applicable instances have been provided. Select *Next* to continue.

Theft/Diversion-CW/CWP COI:

If the user indicates that a Theft/Diversion-CW/CWP was the primary security issue, the user is asked to identify the primary COI and then provide detailed information about each chemical at the asset.

If the user indicates that a Theft/Diversion-CW/CWP is associated with the asset (but is not the primary security issue), the user is asked detailed information about each CW/CWP at the asset.

If no Theft/Diversion-CW/CWP is associated with this asset, the user will not see the CW/CWP COI screen.

If the user indicates that this Asset's Primary Security Issue is a Theft/Diversion CW/CWP:
Indicate the Primary COI for this asset [Q:3.47-8860] 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 COI that should be the primary COI will need to be defined as multiple assets.

For each Theft/Diversion-CW/CWP at the asset:

Is the facility's largest inventory of the COI at this asset? [Q:3.47-9008] Answer *Yes* if the asset contains the largest inventory of the COI.
Is the COI shipped offsite from this asset? [Q:3.47-5532] Answer *Yes* if the COI is shipped offsite from this asset.

Select *Next* to continue.

If the user indicates that this Asset's Primary Security Issue is a Theft/Diversion-CW/CWP, the following questions will be asked about the primary COI.

COI concentration range [Q:3.48-9011] Use the drop-down list to select the concentration range of the COI in this packaging type (% by weight).
Packaging type description [Q:3.48-9031] Enter a brief description of the packaging type. Possible examples of transportation packaging include:

- Bottles
- Totes
- Carboys
- Boxes
- Drums
- Pressurized portable tanks and cylinders

Transportation packaging type [Q:3.48-9032] Use the drop-down list to select the transportation packaging type.
Total quantity of COI in this transportation packaging type (lbs) [Q:3.48-9091] Enter the total quantity for this packaging type.

For chemicals that have multiple concentrations and/or transportation packaging types at this asset, enter the first instance and complete the related questions. Then click *Add*. A new entry line will appear for additional instances. Continue adding entries until all applicable instances have been provided. Select *Next* to continue.

Sabotage/Contamination COI:

If the user indicates that Sabotage/Contamination is the primary security issue, the user is asked to identify the primary chemical and then provide detailed information about each chemical at the asset.

If the user indicates that a Sabotage/Contamination Chemical is associated with the asset (but not the primary security issue), the user is asked detailed information about each Sabotage/Contamination COI at the asset.

If no Sabotage/Contamination Chemical is associated with this asset, the user will not see the Sabotage/Contamination COI screen.

If the user indicates that this Asset's Primary Security Issue was Sabotage/Contamination indicate the Primary COI for this asset [Q:3.53-8864] 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.

For each Sabotage/Contamination COI at the asset:
Quantity [Q:3.53-3632] Enter the quantity (in pounds) at this asset.
Is the facility's largest inventory of the COI at this asset? [Q:3.47-9008] Answer *Yes* if the asset contains the largest inventory of the COI.

Select *Next* to continue.

4.2.3 Initial Identification of Cyber Control and Business Systems:

This screen asks the user to identify if there is a Cyber Control System in place for the asset.

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. Possible examples of these types of systems include SCADA systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS).

Answer *Yes* or *No* to the following question.
Is there a cyber control system related to this asset? [Q:3.56-3659]

Select *Next* to continue.

If the user indicates that this Asset's Primary Security Issue is Theft/Diversion

This screen asks the user to identify if there is a Cyber Business System in place for the asset.

A cyber business system is an information system that is intended to improve the competitive position of an organization or support the corporate strategy of an organization.

Answer *Yes* or *No* to the following question.
Is there a cyber business system related to this asset? [Q:3.561-4292]

Select *Next* to continue

4.2.4 Asset Complete

The last screen asks the user if all the questions were complete for the asset.

Asset Characterization Completed [Q:3.57-4752] If all asset characterization information is complete, check the box and select *Next* to continue. As a reminder, when the user indicates that the questions are complete, they will return to the list of assets. If the user marked the asset complete and all required questions were answered for that asset, the asset will be displayed with a green check mark icon. If the user does not check the box to indicate that the questions are complete, or if any required questions were not answered, the item will be displayed with a yellow warning icon as a reminder that the item is incomplete. The user can reference the green check mark or yellow warning icon as reminders of the status of each item.

Select *Next* to return to the Asset screen. The Asset should now be listed as *Complete*.

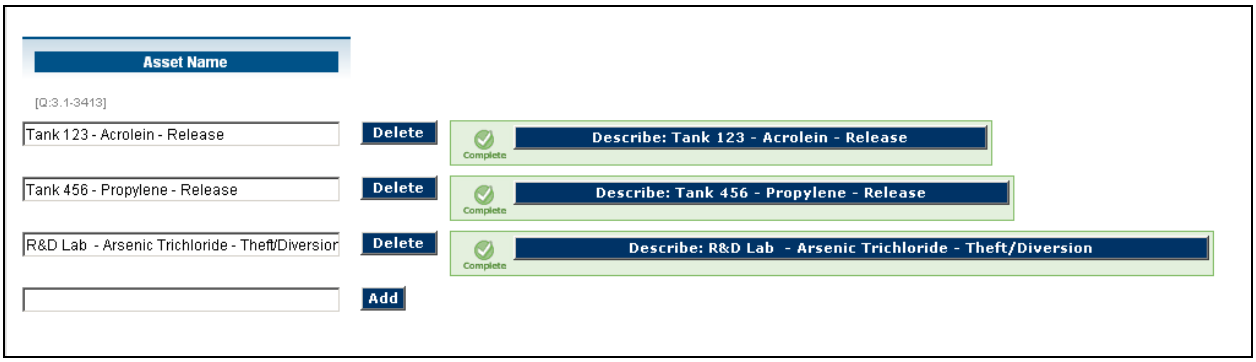

Figure 4-6 Completed Asset Screen

Repeat this process for each facility asset. When all asset descriptions have been completed, answer the question at the bottom of the screen.

Have all assets been listed and described? Once all facility assets have been entered and the detailed information completed, select *Yes* and click *Next* to continue.

4.3 Cyber Control Systems

If the user indicated that the facility has at least one Cyber Control System associated with one or more asset, the following pages will be displayed.

On this screen, the user is asked to identify cyber control systems for assets. These cyber control systems should be limited to those systems that have the ability to control the process and could result in a release or contamination. Possible examples of these types of systems include SCADA systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS).

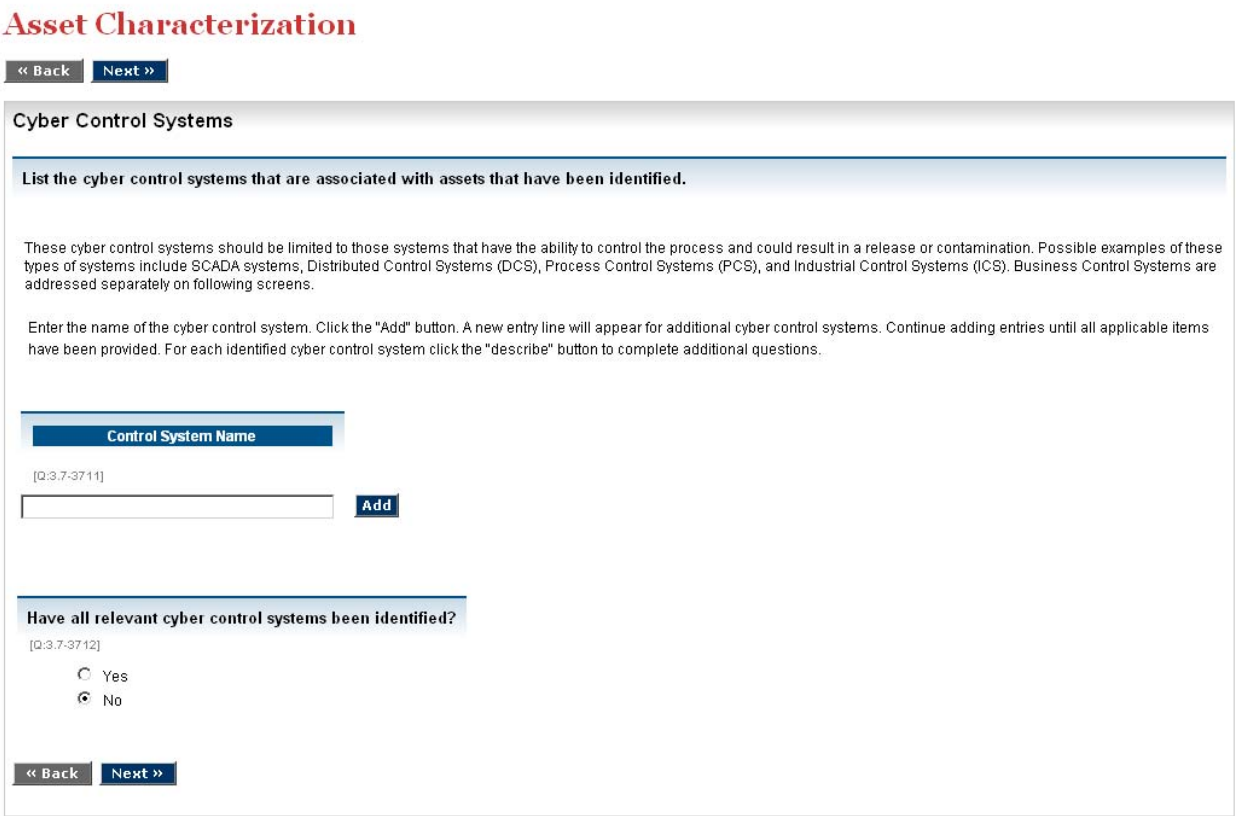

Figure 4-7 Cyber Control Systems Screen

Control System Name: [Q:3.7-3711] Enter the name of the cyber control system. Click the *Add* button. A new entry line will appear for additional cyber control systems. Continue adding entries until all applicable items have been provided. For each identified cyber control system, click the *Describe* button to complete additional questions.

Enter cyber control system description.[Q:3.71-3719].

Is the asset controlled with this control system? [Q:3.71-3835]. 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.

Select *Next* to continue. The user will be returned to the **Cyber Control System** main screen.

Have all relevant cyber control systems been identified? [Q:3.7-3712] Once all of the relevant cyber control systems have been identified, select *Yes* and click *Next* to continue.

4.4 Cyber Business Systems

If the user indicated that the facility has Cyber Business Systems, the following pages will be displayed.

On this screen, the user is asked to identify cyber business systems associated with the assets. Possible examples of these types of systems include business management systems like SAP™ or inventory management systems.

Business System Name [Q:3.8-3715] Enter the name of the cyber business system. Click the *Add* button. A new entry line will appear for additional cyber business systems. Continue adding entries until all applicable items have been provided. For each identified cyber business system, click the *describe* button to complete additional questions.

Enter cyber business system description.[Q:3.81-3720] Provide a description of the cyber business system.

Answer *Yes* or *No* to the following question
Is the asset associated with this business system? [Q:3.81-3837] The bottom section of the screen will show the assets identified earlier in the **Asset Characterization** section. Select *Yes* or *No* to associate the individual asset with the business system. A business system can be associated with multiple assets.

Select *Next* to continue. The user will be returned to the Cyber Business System main screen.

Have all cyber business systems been evaluated? [Q:3.8-3716] Once all of the relevant cyber business systems have been identified, select *Yes* and click *Next* to continue.

This completes **Asset Characterization**. Users will move automatically to the **Vulnerability Analysis** screens.

5.0 Vulnerability Analysis

5.1 Summary of Facility Vulnerability

This section of the SVA Instructions allows the facility to provide input regarding the vulnerability of the facility 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."

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.

5.2 Facility Security Issues to Be Analyzed

The first screen in the **Vulnerability Analysis** section is a summary page highlighting the assets and security issues. The information on this page should be reviewed for accuracy.

A screen shot illustrating this summary information is presented below.

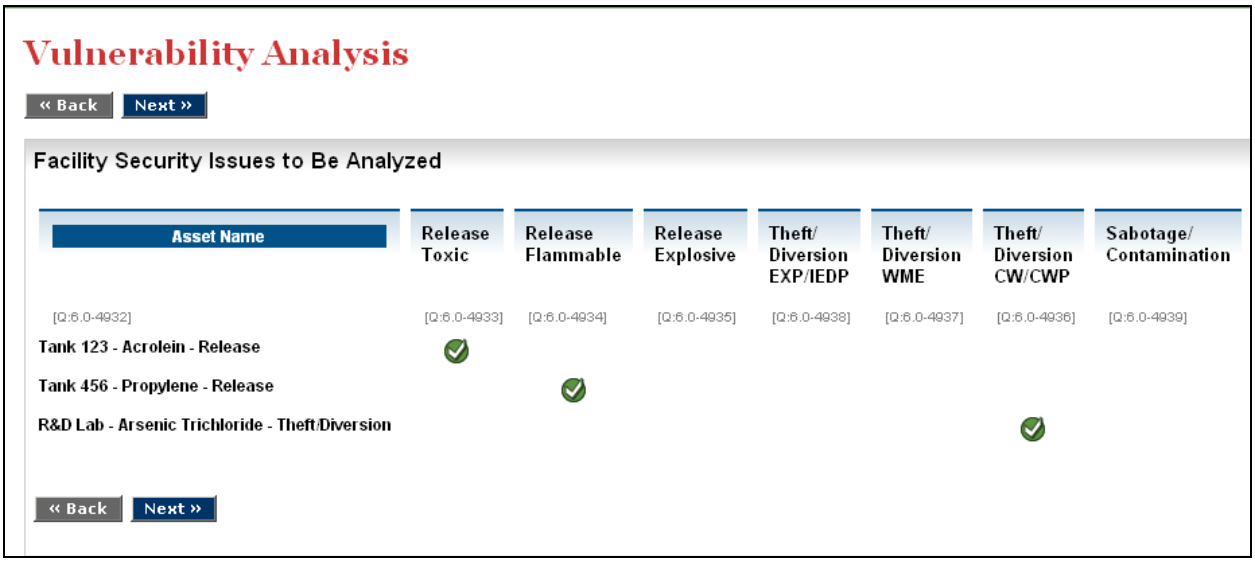

Figure 5-1 Summary of Facility Security Issues to be Analyzed Screen

Once the summary is reviewed, the user clicks *Next* to begin the **Vulnerability Analysis** on each listed Asset.

5.3 Introduction Screen

This Vulnerability Analysis sequence follows the same flow and logic of earlier sections. The user is presented with the assets identified earlier and for each will need to:

- Locate the asset on the facility map
- Complete the Attack Modes relevant to the Asset
    - For each Attack Mode the user will need to select the most relevant attack scenario and answer vulnerability questions.

To begin the Vulnerability Analysis on an asset click on the *Describe* button. This directs the user to the Asset Location Screen.

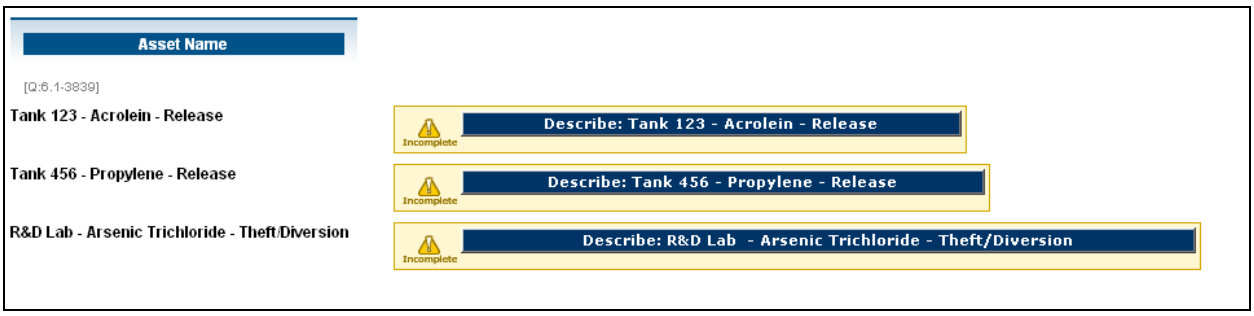

Figure 5-2 Describe Asset for Vulnerability Analysis Screen

5.4 Asset Location

This screen allows the user to identify the location of the asset on an interactive aerial map of the facility and the immediately surrounding area. The user should familiarize themselves with the map navigation features prior to locating the asset. There are two primary features to assist the user with map navigation: the Map Tool Bar (see Figure 5-3) and the associated Map Help table (see Figure 5-4).

Zoom In	Zoom Out	Pan	Full Extent	Locate Asset

Figure 5-3 – Map Tool Bar to Locate Asset

The user may need to navigate within the map to find the asset by using the *Pan* function. This is accomplished by clicking on *Pan* and engaging the directional function by clicking on the map and "dragging" to the desired area.

When the user has located the general area containing the asset, increased magnification is usually required. Increase magnification by clicking on the *Zoom In* button and drawing a rectangle (or successive rectangles) until the level of magnification is sufficient to locate the asset easily.

If additional adjustment is necessary the *Zoom Out* button allows the user to click and drag to a wider localized view. If resetting the full map is desired, simply click the *Full Extent* button to provide the widest view possible and repeat the steps until the asset is clearly identified.

Map Help	
Click a button in the map toolbar to choose a tool. The tools may be used as follows:	
Zoom In	Click and drag to create a rectangle around the area to magnify.
Zoom Out	Click and drag to zoom out.
Pan	Click and drag to view other parts of the map without resizing. The map will move in the direction the user drags.
Full Extent	Click the Full Extent button once to view the magnification that shows the entire map. At the full extent, the user will not be able to zoom out further.
Locate Asset	Click on the map to identify the location of the asset.

Figure 5-4 – Map Help Table

Once the user is satisfied that the asset has been located, click on *Locate Asset* in the Map Tool Bar. This will place a visible identifier, a pink star ☆ on the map at the asset location. The user then clicks on the *Next* button to proceed with the vulnerability analysis.

Note: Do NOT click the *Next* button at the bottom of the screen until the star appears on the map.

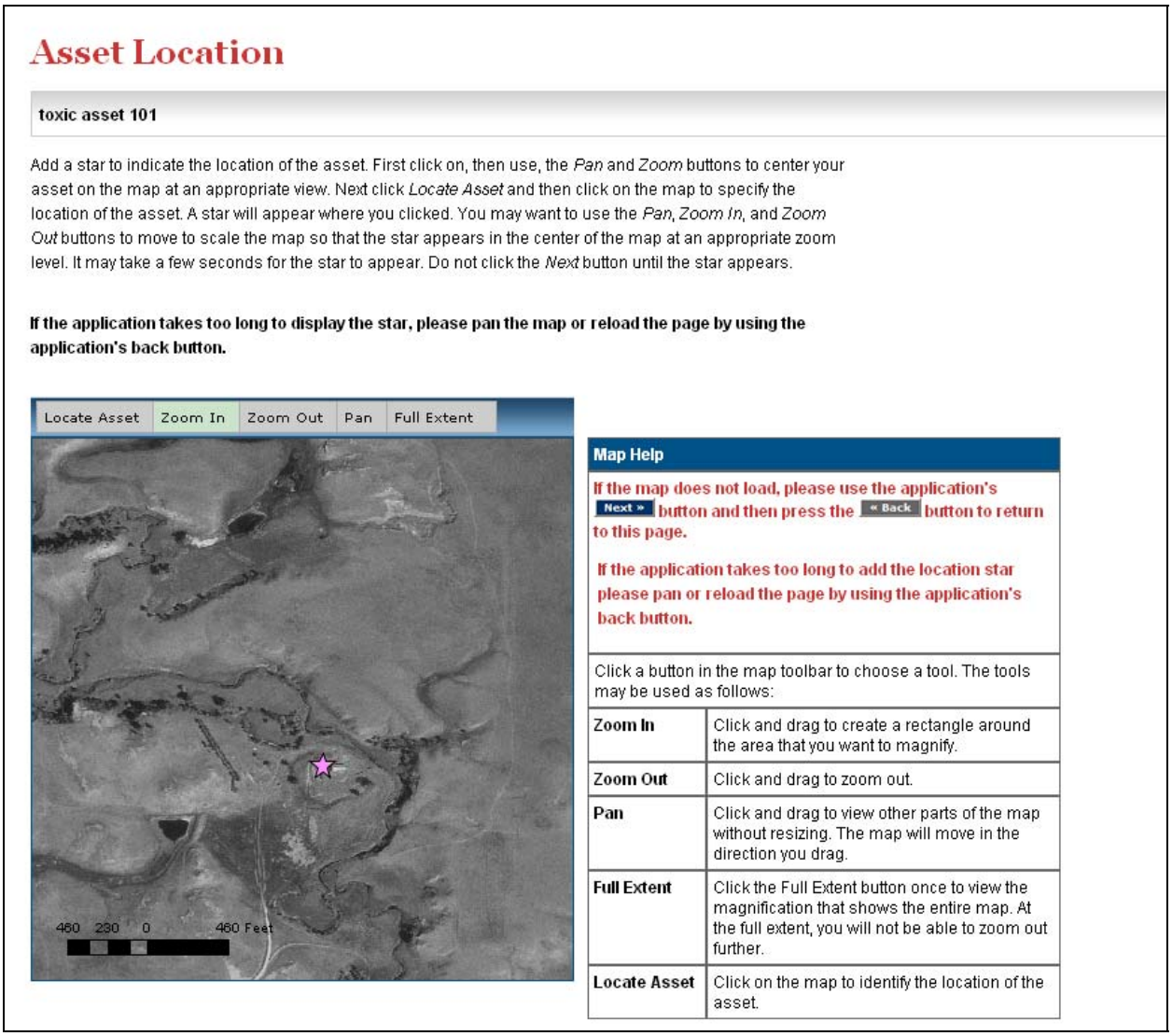

Figure 5-5 Locate Asset Screen

5.5 Attack Mode Screen

Once the asset has been successfully located, the user should click on the *Next* button to move to the **Attack Mode** screen. For each asset, only the Attack Modes that pertain to that asset will appear (e.g., a facility not on a navigable waterway will not need to answer Maritime Scenario questions). Up to seven attack modes are possible:

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

- Assault Team
- Standoff

Each set of attack mode screens works similarly. The user will see the map image of the asset for reference and will need to:

- **Select an Attack Scenario**
  The user 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 arrangement and security systems. Detailed descriptions of the attack scenarios are available online at csat.dhs.gov/csat.

- **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. For Maritime, Vehicle and Standoff scenarios, an attack location will need to be identified by the facility. For Aircraft and Assault scenarios, the attack location is assumed to be the center of the asset.

  Damage circles will display on the map to provide the facility with a visual reference for answering the vulnerability factors.

  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

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

- **Attack Scenario Questions**
  For Maritime, Vehicle and Standoff scenarios the user must determine if the asset is within the inner damage circle. If the asset is not within the inner damage circle, the vulnerability analysis will be complete at this point. (e.g., a navigable waterway was identified, but an attack from the waterway would not affect the asset, so the vulnerability analysis is complete). If the asset is within the outer damage circle or the user is completing an Aircraft or Assault Team scenario, the user will need to determine the population within the inner damage circle.

  When completing a Theft, Diversion, or Sabotage scenario, the user will only answer questions on the primary COI at risk.

- **Vulnerability Factors**
  For each attack scenario, the user will see a series of vulnerability factor questions; these questions will vary depending on the attack scenario.

- **Release Questions**
  For release scenarios, the user will answer some specific release questions.

To begin, click on the first *Attack Scenario* button and complete the questions. When an attack scenario is completed, the user will be returned to the Attack Scenario Screen. The *Attack Scenario* button will now be green and display a *Complete* status. The user then clicks on the next scenario to continue the analysis.

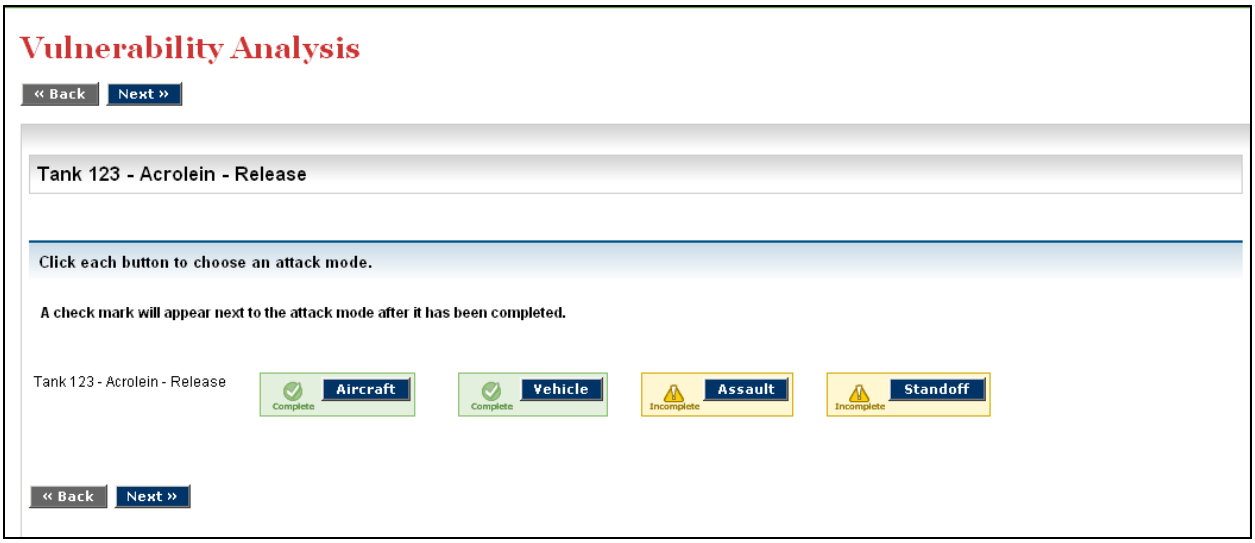

Figure 5-6 Attack Scenario Screen

5.5.1 Select Attack Scenario

The user should use the radio buttons to select an attack scenario. 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.

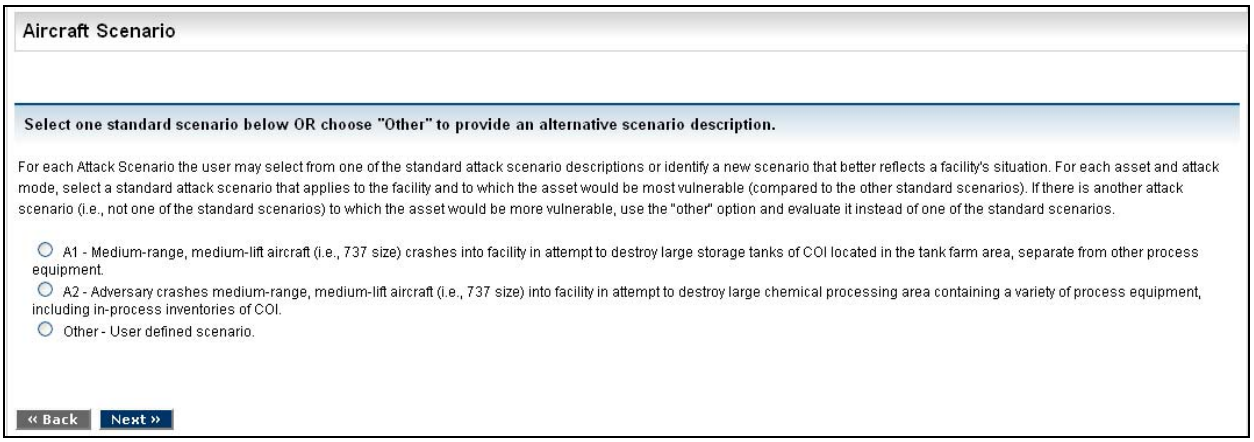

Figure 5-7 Aircraft Attack Scenario Screen

Brief Descriptions of the Standard Attack Scenarios

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.

Vehicle Borne Improved Explosive Device (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.

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 7ft. 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.

Detailed descriptions of the attack scenarios may be found in the CSAT SVA Attack Scenario Descriptions, available online at csat.dhs.gov/csat to active CSAT users that have completed CVI training and have started their SVA.

If *other* was selected for attack scenario, the user will be asked to:
Describe the attack scenario relevant to this asset. [Q:9.01-7588, Q:7.01-7275, Q:8.01-7563, Q:10.01-7613, Q:11.01-7631, Q:12.01-7656, Q: 13.01-9938] This should include information such as the assumed point of attack and sequence of events.

5.5.2 Attack Location Map

For Maritime, Vehicle and Standoff attack scenarios, an attack location will need to be identified. For Aircraft and Assault scenarios, the attack location is assumed to be the center of the asset.

For Maritime, Vehicle, and Standoff attack scenarios, the Map Tool Bar changes to reflect *Locate Attack Location*; however, the navigational functionality is the same as the earlier map screens. After the aerial photo appears, the user clicks on the *Locate Attack Location* button and then clicks on the map in the area near the asset location to identify the attack location that will achieve the maximum damage, by including the asset and other collateral sub-targets to generate the greatest consequence.

Specifically:

- If the primary COI of the asset being attacked is a release-toxic, 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, 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, identify the location of the attack that results in the greatest amount of release-explosive COI released.

For a Maritime attack, the location will need to be on a navigable waterway (i.e., not on land).

Locate Attack Location	Zoom In	Zoom Out	Pan	Full Extent

Figure 5-8 Map Tool Bar to Locate Attack Location

The user should identify and evaluate attack locations with a high potential consequence by clicking on the *Locate Attack Location* button and waiting for the damage circles to appear.

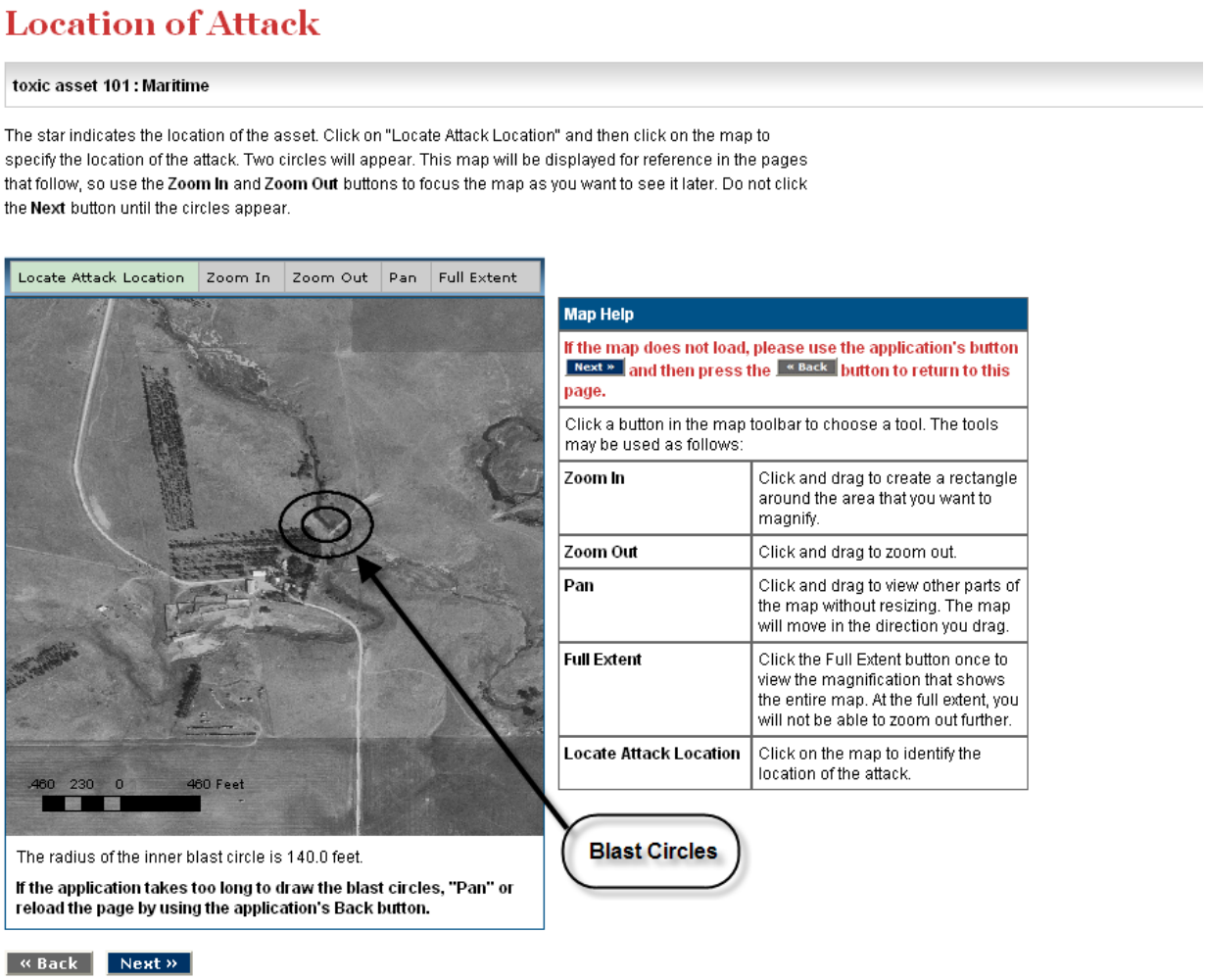

Figure 5-9 Map of Asset with Blast Circles

Note: A Maritime attack needs to be placed on a Navigable Waterway, even if the asset is not located within the blast circles.

Note: Do NOT click the *Next* button at the bottom of the screen until the blast circles appear on the map.

Zoom in around the blast circles. This image will appear on the next page for reference but printing this page is also suggested. Click the *Next* button to proceed with the vulnerability analysis.

5.5.3 Attack Scenario Questions

For Maritime, Vehicle and Standoff attack scenarios, the user must determine if the asset is within the inner damage circle. Use the map with the damage circles to determine the answer to the following question:

> **Maritime: Is any portion of the asset within the inner damage radius (140 feet)?**[Q:7.2-1531]
> **Vehicle: Is any portion of the asset within the inner damage radius (170 feet)?** [Q:8.2-9626]
> **Standoff: Is any portion of the asset within the range of the standoff weapon (657 feet)?** [Q:11.2-10337]
>
> For these specific scenarios, there MAY be situations when physical constraints (e.g., no waterway near asset) have the result that an asset CANNOT be included within some portion of the inner damage circle. In this case, the user would mark the *No* circle; however, in most cases the user would check the *Yes*.
>
> The user then clicks on the *Next* button to continue with the analysis. If an asset is located within the inner damage circle, the user will be directed to further attack screens. If no assets are located in the inner damage circle, the user is directed to conclude the Attack Consequence analysis.

For all Aircraft and Assault attack scenarios, and the qualifying Maritime and Vehicle scenarios, users answer population questions. The number 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, such as during turnarounds, in this number.

> **Maritime: What is the expected number of people at the facility within the outer damage radius (270 feet)?** [Q:7.21-3896]
> **Vehicle: What is the expected number of people at the facility within the outer damage radius (340 feet)?** [Q:8.21-3995]
> **Aircraft: What is the expected number of people at the facility within the outer damage radius (950 feet)?** [Q:9.21-4063]
> **Assault: What is the expected number of people at the facility within the outer damage radius (110 feet)?** [Q:10.21-4080]

For a Diversion scenario, the user will be asked:

> **Is the customer permitted to pick up orders at this asset?** [Q:12.6-7736] This will determine which vulnerability factor questions are asked later.

For Theft, Diversion and Sabotage attack scenarios, the user answers questions on the material at risk. This COI is listed on the screen.

> **Quantity of COI at Risk in this scenario (pounds).** [Q:12.2-11343, Q:13.2-11372]
> **Percent Concentration by Weight in this scenario.** [Q:12.2-11344, Q:13.2-11373]

5.5.4 Vulnerability Factors Questions

The vulnerability factor questions and wording may differ slightly depending on attack scenario. All questions are listed below, but only applicable ones will appear on screen.

Documenting Assumptions for all Vulnerability Factors

After the user has selected the vulnerability factor value that best represents the vulnerability situation for the attack mode for a specific asset, the user has the opportunity to document any **Assumptions** the user made in assigning that value. The input field is a text field and is optional. However, providing some information in the Assumption field will help the facility and DHS understand the facility's rationale for the vulnerability factor assignment.

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, a facility should consider it difficult for an adversary to distinguish between several similar items of equipment, only some of which would be viable targets. Labeling of equipment is also a factor in this assessment.

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? [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]
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)

Identifiability assumptions [Q:7.22-7277, Q:9.22- 9688,Q:8.22-9610, Q:10.22-9768, Q:11.22-9901, Q:12.22-7658, Q:13.22-9949] Document any important assumptions made in assessing identifiability.

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 (not counting facility or offsite security force response capability).

This factor should reflect the ability of existing security systems and processes (without counting for response force actions) 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).

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? [Q:7.22-7371, Q:8.22-9611, Q:10.22-9769, Q:11.22-9902, Q:12.22-7659, Q:13.22-9950]
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)

Accessibility assumptions [Q:7.22-7372, Q:8.22-9612, Q:10.22-9769, Q:11.22-9903, Q:12.22-7659, Q:13.22-9951] Document any important assumptions the SVA team made in assessing accessibility.

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 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 discussed above would not have stopped the adversary, but would have offered a delay consistent with the types of physical security measures at the facility.

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)? [Q:7.22-7391, Q:8.22-9613,Q:10.22-9771, Q:12.22-7661, Q:13.22-9952] 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)

Facility security response force capability assumptions [Q:7.22-7411, Q:8.22-9614, Q:10.22-9772, Q:12.22-7662, Q:13.22-9953]

Document any important assumptions made in assessing facility security response force capability.

Offsite Security Response Force Capability

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 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). Also, 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.

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)? [Q:7.22-7412, Q:8.22-9615, Q:10.22-9773, Q:12.22-7663, Q:13.22-9954] 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)

Offsite security response force capability assumptions [Q:7.22-7413, Q:8.22-9616, Q:10.22-9774, Q:12.22-7664, Q:13.22-9955] Document any important assumptions made in assessing offsite security response force capability.

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 less than 1.0 could include:

- Inaccuracy of a standoff weapon
- Difficulty in attacking a point target with the specified aircraft (particularly if the asset is among many other pieces of equipment or units)
- Difficulty in loading a large but portable package
- Difficulty in effectively contaminating a COI shipment

How likely is the adversary to succeed in accomplishing this attack (giving no credit for any facility or asset security measures)? [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] 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)

Achievability assumptions [Q:7.22-7415, Q:9.22-9690, Q:8.22-9618, , Q:10.22-9776, Q:11.22-9905, Q:12.22-7666, Q:13.22-9957] Document any important assumptions made in assessing achievability.

Target Hardness Probability

This refers to the probability that an adversary that 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.

Do not give additional credit for considerations you have already credited in evaluation of earlier factors (e.g., achievability, identifiability). This factor represents the inherent hardness or location of the target that protects it from the effects of an attack that was successfully initiated. Examples of situations where credit could be assessed include:

- 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.
- A vessel with multiple layers or insulation that provides spacing such that a standoff weapon would not be effective in penetrating the vessel.
- Hardware approaches that make theft of portable containers very difficult even when access is achieved.
- 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.

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? [Q:7.22-7416, Q:8.22-9619, Q:10.22-9777, Q:11.22-9906, Q:13.22-9958] 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 to 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)

Target hardness assumptions. [Q:7.22-7417, Q:8.22-9619, Q:10.22-9778, Q:11.22-9907, Q:13.22-9959] Document any important assumptions made in assessing target hardness.

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 not readily available to the adversary. For example, select *Attack is extremely unlikely to occur at a time the asset contains a significant quantity of the COI* for a batch process tank that only contains the COI for one hour every 24 hours, on a schedule not available or visible to the adversary.

The Primary COI is listed here, as it is the applicable COI referred to in the Availability Probability questions.
How likely is the specific asset attacked to contain the relevant COI, assuming that the adversary identifies and attacks the correct target asset?[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]
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)

Availability assumptions. [Q:9.22-9695, 7.22-8912, Q:8.22-9625, Q:10.22-9783, Q:11.22-9912, Q:12.22-9362, Q:13.22-9962] Document any important assumptions made in assessing availability.

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 and will only be shown for the Diversion Scenario.

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) 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 itself as an approved customer.

How likely is the adversary to be able to register as a new customer that is approved to purchase theft/diversion COI? [Q:12.8-7682] 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)

Unauthorized customer registration assumptions. [Q:12.8-7682] Document any important assumptions made in assessing unauthorized customer registration.

Unauthorized Order Placement

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's (adversary) 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 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. It will only be shown for the Diversion scenarios.

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? [Q:12.8-7684] 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)

Unauthorized order placement assumptions [Q:12.8-7685] Document any important assumptions made in assessing unauthorized order placement.

Unauthorized Order Pick Up

This refers to the probability that an adversary could pick up an order being held for an authorized customer, and will only be shown for the Diversion scenarios when the facility allows customer pick up.

This vulnerability assumes that the adversary has not been able to place an order. The ability of the adversary to pick up an authorized customer's order could result, for example, from a facility's failure to secure its shipping and receiving. Another possible factor in this assessment is the trustworthiness of the facility personnel involved in the physical packing, staging and shipping processes.

How likely is the adversary to be able to pick up an order for an authorized customer for this COI? [Q:12.8-7686] 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)

Unauthorized order pick up assumptions. [Q:12.8-7687] Document any important assumptions made in assessing unauthorized order pick up.

For Theft/Diversion and Sabotage scenarios the vulnerability analysis for this asset is complete. Clicking *Next* will ask the user to confirm completion and return the user to select another Scenario.

5.5.5 Release Questions

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

Calculate the quantity using the same counting rules provided by CFATS for calculating the STQs for the applicable release chemicals of interest.

Quantity (pounds) within the inner damage radius.

- If the primary COI is a release-toxic, 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:7.3-9170, Q:8.3-9636, Q:9.3-9706, Q:10.3-9793]

- If the primary COI is a release-flammable, 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:7.4-9226, Q:8.4-9668, Q:9.4-9738, Q:10.4-9825]

- If the primary COI is a release-explosive 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:7.5-9228, Q:8.4-9673, Q:9.5-9743, Q:10.5-9830]

Mitigation Factors
If the Primary COI is a release-toxic the user was asked about mitigation factors during the Asset Characterization section (Section 4.2.2). If any mitigation factors were identified, the user will be asked if the mitigation factor would survive the attack. If no mitigation factors were included, no questions will display.

Does the dike or berm containment survive the attack? [Q:7.3-9177,Q:8.3-9637,Q:9.3-9707, Q:10.3-9794, Q:11.3-9974]
Does the leak detection system survive the attack? [Q:7.3-9191, Q:8.3-9638,Q:9.3-9708, Q:10.3-9795, Q:11.3-9975]
Does the fixed vapor suppression system survive the attack? [Q:7.3-9192, Q:8.3-9639,Q:9.3-9709, Q:10.3-9796, Q:11.3-9976]
Does the offsite notification system survive the attack? [Q:7.3-9193, Q:8.3-9640,Q:9.3-9710, Q:10.3-9797, Q:11.3-9977]
Does the other mitigation measure survive the attack? [Q:7.3-9194, Q:8.3-9641, Q:9.3-9711, Q:10.3-9798, Q:11.3-9978]

5.5.6 Vulnerability Analysis Complete

The vulnerability analysis for this asset is complete. Clicking *Next* will ask the user to confirm completion and then return the user to select another Scenario. As a reminder, when the user indicates that the questions are complete, they will return to the list of attack scenarios and this item will be marked as complete with a green check mark icon. If the user does not check the box to indicate that the questions are complete, the item will be displayed with a yellow warning icon. The user can reference the green check mark or yellow warning icon as reminders of the status of each item.

Have vulnerability assessments been completed for all attack scenarios for all assets? [Q: 6.1-1396] When all scenarios are complete for all assets, the user has completed the vulnerability analysis portion of the SVA. Check *Yes*.

Clicking *Next* will direct the user to the **Computer Systems Analysis** section.

6.0 Computer Systems Analysis

When the **Vulnerability Analysis** is complete, the user will continue to the **Computer Systems Analysis** section, or may choose the option from the menu on the left side of the screen.

The user will need to use the radio buttons to select the appropriate response to the computer analysis questions.

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.)? [Q:14.09-4151]

Are personnel screened at facility entrances for unauthorized cyber related equipment? [Q:14.09-4152]

Has the personnel screening process been validated through testing by professional security services? [Q:14.091-4153]

6.1 Cyber Control Systems

If any cyber system were identified earlier in the SVA, the Computer Control screen will be shown. The user will need to answer the series of questions by selecting ***Describe <computer system name>*** for each computer control system listed.

6.1.1 Map Cyber Control System

Similar to the mapping done earlier, the computer control system should be identified on the map.

On the Computer Control screen the Map Tool Bar has been changed to reflect *Locate System*, (see Figure 6-1 below) however the navigational functionality is the same as the earlier mapping screens. After the aerial photo appears, the user clicks on the *Locate System* button and then clicks on the map to identify where the control system is located.

Zoom In	Zoom Out	Pan	Full Extent	Locate System

Figure 6-1– Map Tool Bar to Locate System

Once the Cyber Control system location has been identified on the map, click *Next*.

6.1.2 Cyber Control System Questions

Finish the Computer Security Analysis by completing the questions on the next series of screens.

Is external access (e.g., Internet, modem, wireless) to cyber systems allowed? [Q:14.3-1614]

Has the lack of external access been validated through testing by IT security professional services? [Q:14.31-1633]

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:14.32-1635]

Has the disabling of communication capabilities been validated through testing by a professional IT security service? [Q:14.33-1637]

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:14.34-1692]

Does the facility have a documented and distributed cyber change management policy and supporting procedures (e.g., new hardware/software, employee access)? [Q:14.34-1693]

Has an individual(s) been designated as responsible for cyber security at the facility? [Q:14.34-1694]

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:14.34-2851]

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:14.34-1695]

Have all default passwords been changed to user-specific passwords? [Q:14.34-1696]

Are accounts locked out after several unsuccessful login attempts? [Q:14.34-1697]

Personnel Security

Does the facility perform background checks for personnel in critical/sensitive positions? [Q:14.35-1719]

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:14.35-1720]

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:14.35-1721]

Awareness and Training

Does the facility provide cyber security training? [Q:14.35-1723]

Monitoring and Incident Response

Does the facility log cyber security events on systems and review them on a regular basis? [Q:14.36-1727]

Does the facility log cyber security events on servers, and review them on a regular basis? [Q:14.36-2852]

Does the facility report significant cyber security events to senior management? [Q:14.36-1728]

Does the facility mandate malicious code protection on all systems? [Q:14.36-1730]

Does the cyber system allow email? [Q:14.37-1735]

Are email attachments (e.g., executable files) filtered on incoming email? [Q:14.38-1737]

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:14.39-1175]

Configuration Management

Has a business requirement been established for every external connection into the network/ environment, including wireless and modem connections? [Q:14.4-1741]

Does the facility apply/perform regular software and hardware, patches, updates, upgrades, and replacements? [Q:14.4-1742]

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:14.4-1743]

Risk and Vulnerability Management

Have potential vulnerabilities of critical assets, systems, and networks been identified and evaluated? [Q:14.4-2854]

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:14.4-1744]

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:14.4-2855]

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)? [Q:14.4-2856]

When all the questions about the Cyber Control System have been answered, check the box next to: **Cyber Control System Complete**.

The user will be returned to the Cyber Control System screen and can complete information for any additional control systems.

Once all cyber systems have been described, the user will check *Yes* next to: **Have all cyber control systems been evaluated?** [Q:14.1-4157].

6.2 Business Control Systems

If any business system were identified earlier in the SVA, the Business Control screen will be shown. The user will need to answer the series of questions by selecting ***Describe <computer system name>*** for each business system listed.

Answer *Yes* or *No* to the question: **Is this cyber system physically located at the facility?** [Q:14.61-4175].

If the answer is *Yes*, the user will be asked to map its location. If the answer is *no*, the user will be asked to identify where the system is located.

6.2.1 Map Business Control System

Similar to the mapping done earlier, the business control system should be identified on the map.

On the Business Control screen the Map Tool Bar has been changed to reflect *Locate System*, (see Figure 6-2 below) however the navigational functionality is the same as the earlier mapping screens. After the aerial photo appears, the user clicks on the *Locate System* button and then clicks on the map to identify where the business system is located.

Zoom In	Zoom Out	Pan	Full Extent	Locate System

Figure 6-2– Map Tool Bar to Locate System

Once the Business Control system has been identified on the map, click *Next*.

Finish the Computer Security Analysis by completing the questions on the next series of screens.

6.2.2 Locate Business System Not at Asset

Select the Country [Q:14.62-8232] Identify the country in which the business system is located, by using the drop-down list.

Click *Next* to enter the location of the business system

Enter the cyber system location.
Location/Building Name [Q:14.63-4177]
Street [Q:14.63-4178]
Street Line 2 [Q:14.63-8271]
City [Q:14.63-4179]
State [Q:14.63-4180]
ZIP Code [Q:14.63-4181]

Click *Next* to complete the questions on the next series of screens.

6.2.3 Business System Questions

Is external access (e.g., Internet, modem, wireless) to cyber systems allowed? [Q:14.8-1033]

Has the lack of external access been validated through testing by IT security professional services? [Q:14.81-1034]

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 (PDA's), flash drives, data disks, smart cell phones)? [Q:14.82-1035]

Has the disabling of communication capabilities been validated through testing by a professional IT security service? [Q:14.83-1036]

<u>Security Policy</u>

Does the facility have documented and distributed cyber security policies, plans, and supporting procedures commensurate with the current information technology operating environment? [Q:14.84-1051]

Does the facility have a documented and distributed cyber change management policy and supporting procedures (e.g., new hardware/software, employee access)? [Q: 14.84-1071]

Has an individual(s) been designated as responsible for cyber security at the facility? [Q: 14.84-1072]

<u>Access Control</u>

Does the facility allow systems to have external connections with portable electronic devices configured for minimum business needs and verified with scans? [Q: 14.84-2811]

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: 14.84-1092]

Have all default passwords been changed to user-specific passwords? [Q: 14.84-1093]

Are accounts locked out after several unsuccessful login attempts? [Q: 14.84-1094]

Personnel Security

Does the facility perform background checks for personnel in critical/sensitive positions? [Q: 14.85-1100]

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:14.85-1101]

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:14.85-1105]

Awareness and Training

Does the facility provide cyber security training? [Q:14.85-1107]

Monitoring and Incident Response

Does the facility log cyber security events on systems and review them on a regular basis? [Q: 14.86-1151]

Does the facility log cyber security events on servers, and review them on a regular basis? [Q:14.86-2831]

Does the facility report significant cyber security events to senior management? [Q: 14.86-1152]

Does the facility mandate malicious code protection on all systems? [Q 14.86-1153]

Does the cyber system allow email? [Q: 14.87-1173]

Are email attachments (e.g., executable files) filtered on incoming email? [Q: 14.88-1174]

Configuration Management

Has a business requirement been established for every external connection into the network/ environment, including wireless and modem connections? [Q: 14.9-1191]

Does the facility apply/perform regular software and hardware, patches, updates, upgrades, and replacements? [Q: 14.9-1192]

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: 14.9-1193]

Risk and Vulnerability Management

Have potential vulnerabilities of critical assets, systems, and networks been identified and evaluated? [Q: 14.9-2832]

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: 14.9-1195]

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: 14.9-2833]

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)? [Q: 14.9-2834]

When all the questions about the Business System have been answered, check the box next to: **Cyber Business System Complete**.

The user will be returned to the Cyber Business System screen and can complete any additional business systems.

Once all cyber business systems have been described, the user will check *Yes* next to: **Have all cyber business systems been evaluated?** [Q: 14.6-4172].

Once all the computer security analysis questions have been completed, the user will check the ***Yes*** radio button next to the ***Have all Computer Security Analysis questions been completed?*** [Q:14.48-4753] indicating that all of the appropriate questions have been answered.

Click on the ***Next*** button to complete the survey.

7.0 SVA Completion

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

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

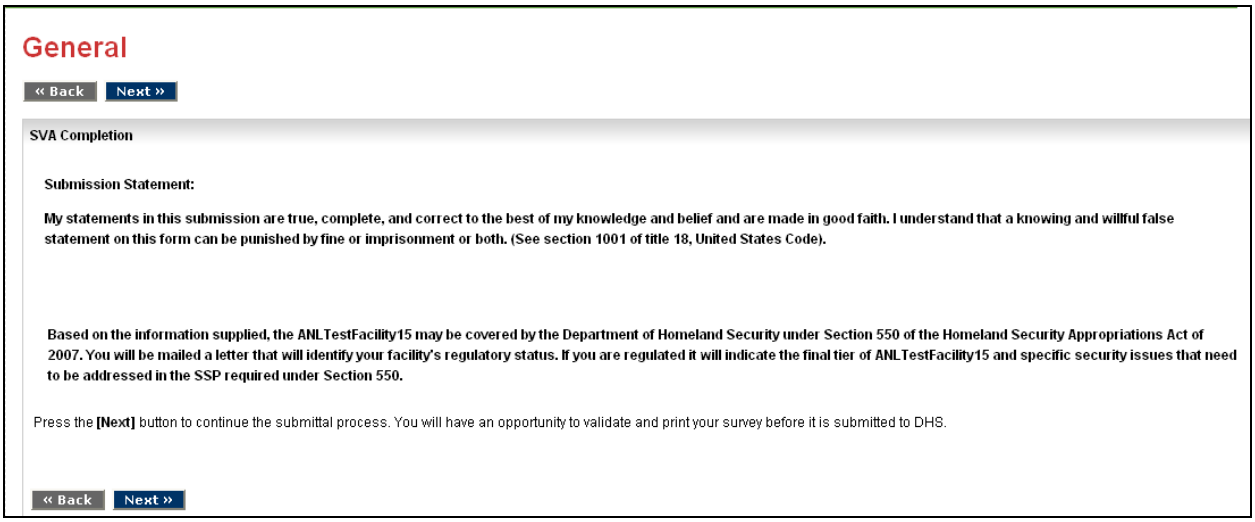

Figure 7-1–SVA Completion

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

View Summary Report. Click on ***View Summary Report*** on the menu on the left and the SVA tool will generate a report showing the questions and the data entered. This report can be printed using the ***Print This Report*** button on the top of the screen or the print function in the browser.

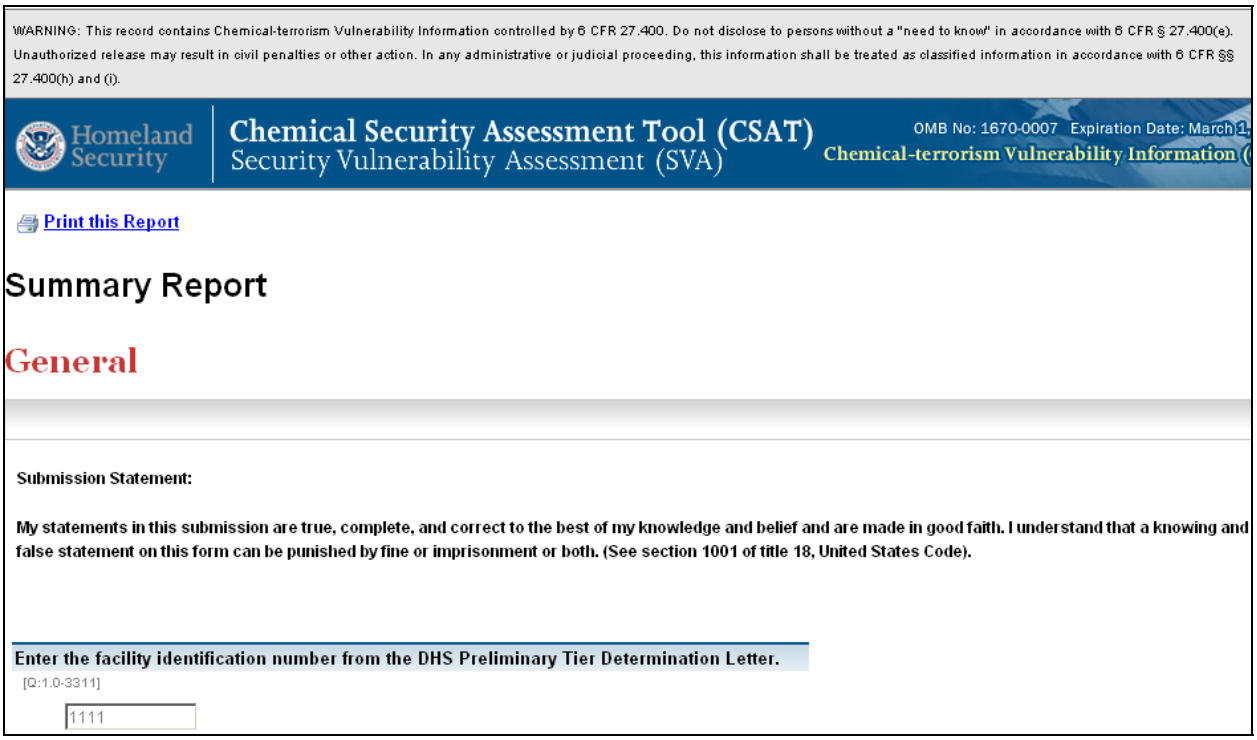

Figure 7-2–Summary Report

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

Note: If the Preparer is also the Submitter, and has only one username, the screen presentation will be similar to the Submitter screens detailed below. The Preparer will not have the option to transfer the account to the Submitter, but will be directed to submit the completed SVA directly to DHS.

Transferring Answers to Submitter. Click the ***Transfer to Submitter for Review*** button to transmit SVA to the Submitter for review. The Preparer can also choose to have a copy of communications from DHS sent to them as well. [Q:1.92-5292] A *Yes* answer will send an email notifying the Preparer that the survey has been transmitted 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 revision (at which point the Preparer may again edit and enter data).

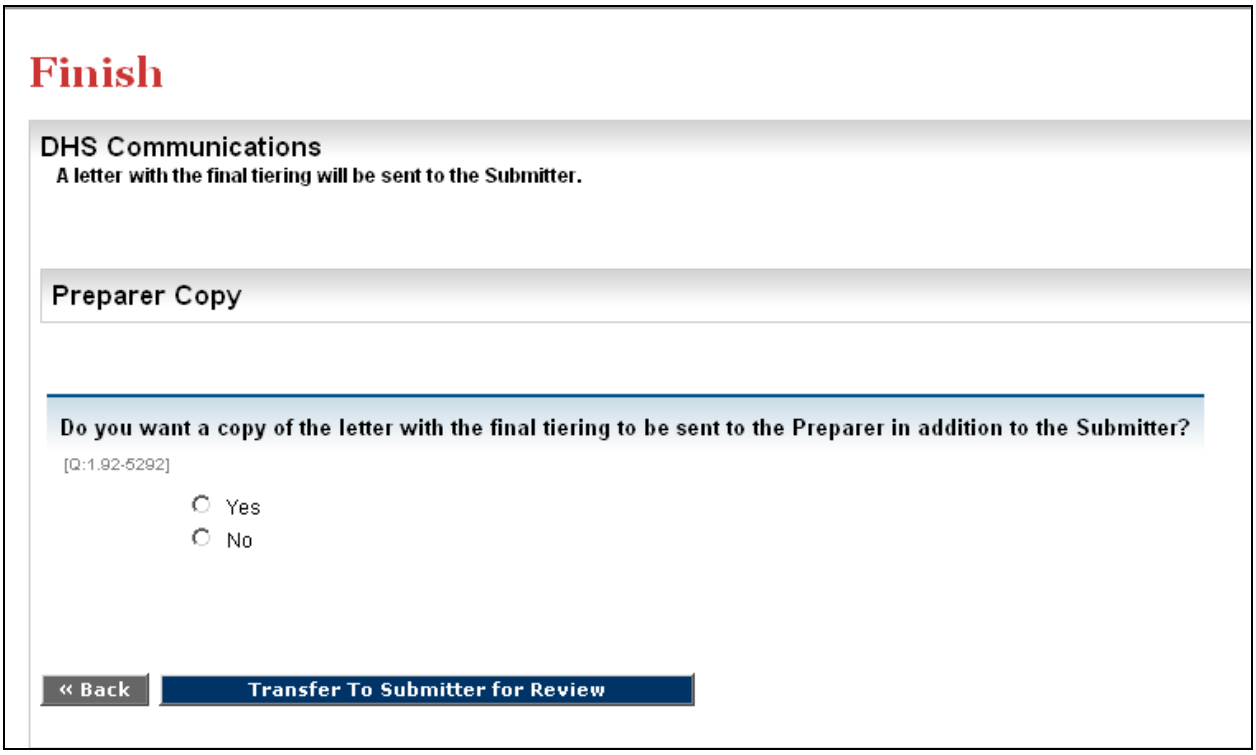

Figure 7-3–DHS Communications – Preparer Screen

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

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

If the SVA is returned to the Preparer, its status will return to *In Progress* on the initial sign-in screen and the Preparer and Submitter will receive emails with instructions.

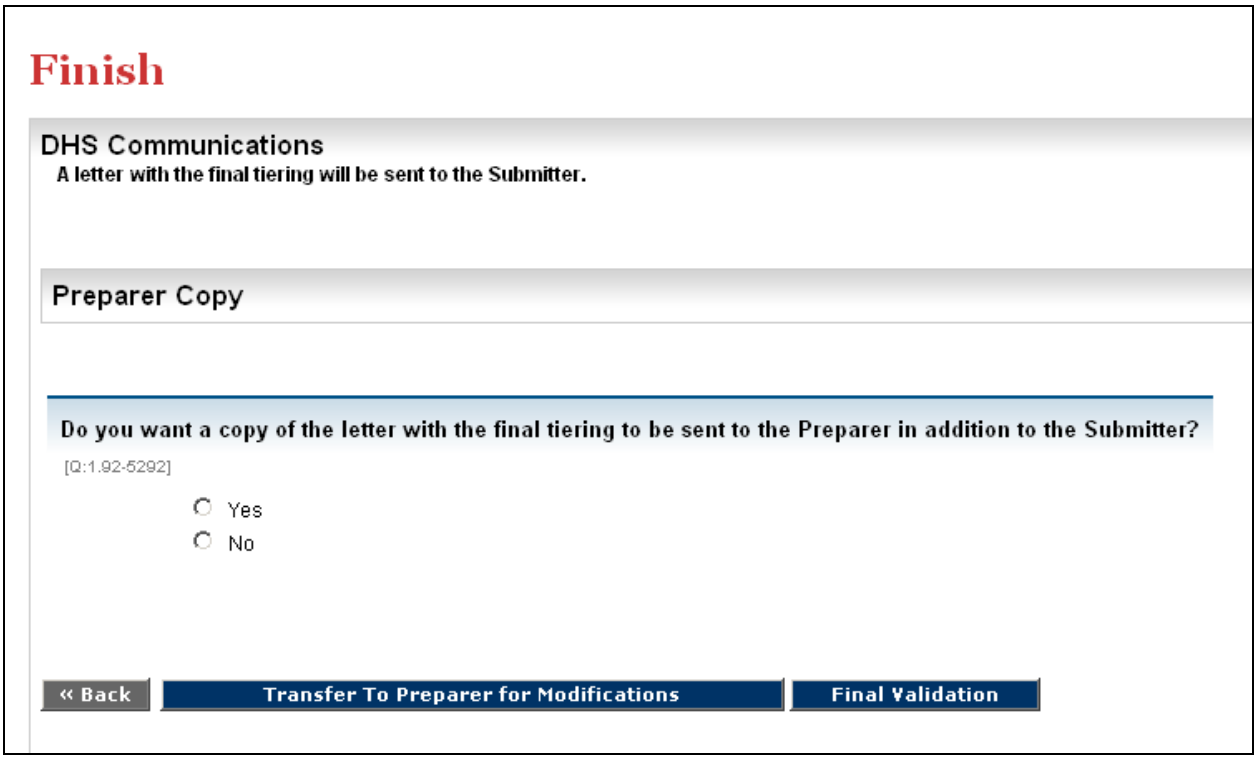

Figure 7-4–DHS Communications – Submitter Screen

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

Figure 7-5–Validation Complete

The Submitter must retain a copy of the completed SVA for the facility's record as specified in 6 CFR §27.255(b). Once the SVA is submitted to DHS, a facility no longer has access to it. A submitted copy of the SVA will be helpful in case the data needs to be re-entered. This printed or electronic record is CVI and must be protected as CVI. Users can create a copy of the completed SVA by clicking on the button ***Print Version of SVA***. After printing a copy for your files, and checking that the copy is legible; the Submitter should click ***Submit to DHS*** to officially submit the completed SVA**.**

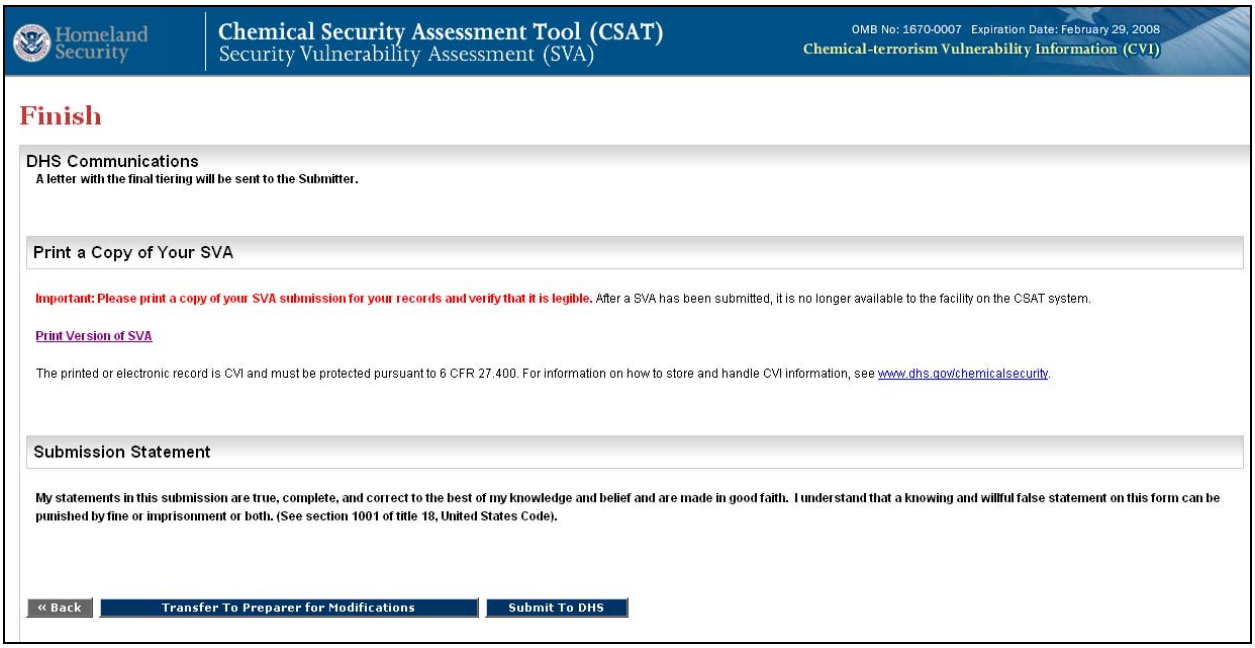

Figure 7-6–Finish

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

SVA Tool Complete

List of Acronyms

ASP	Alternate Security Program
CCPS	Center for Chemical Process Safety
CCTV	Closed-Circuit Television
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
COI	Chemical(s) of Interest
CSAT	Chemical Security Assessment Tool
CVI	Chemical-terrorism Vulnerability Information
CW/CWP	Chemical Weapons/Chemical Weapons Precursor
DCS	Distributed Control Systems
DHS	U.S. Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
EXP/IEDP	Explosive/Improvised Explosive Device Precursor
FAQ	Frequently Asked Question
ICS	Industrial Control Systems
IED	Improvised Explosive Device
IEDP	Improvised Explosive Device Precursor
IFR	Interim Final Rule
IMS	Intrusion Monitoring System
IT	Information Technology
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