Chemical Security Assessment Tool (CSAT) 2.0
Security Vulnerability Assessment / Site Security Plan Instructions

September 30, 2016

Homeland Security

Table of Contents

Security Vulnerability Assessment (SVA) / Site Security Plan (SSP) Requirements

Chemical Facility Anti-Terrorism Standards (CFATS)

On December 18, 2014, the President signed into law the *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014* ("CFATS Act of 2014") providing long-term authorization for the CFATS program. The CFATS Act of 2014 codified the Department of Homeland Security's (DHS or Department) authority to implement the CFATS program into the Homeland Security Act of 2002. See 6 USC § 621 et seq.

Section 550 of Public Law 109-295 previously provided (and the CFATS Act of 2014 continues to provide) the Department with the authority to identify and regulate the security of high-risk chemical facilities using a risk-based approach. On April 9, 2007, the Department issued the CFATS Interim Final Rule (IFR), implementing this statutory mandate. See 72 FR. 17688.

Do I Need to Submit a Security Vulnerability Assessment/Site Security Plan (SVA/SSP)?

You need to submit to DHS an SVA/SSP, an easy-to-use online questionnaire available through CSAT, if your facility is determined to be high-risk, Tier 1-4, after DHS has reviewed your facility's Top-Screen.

You may need to submit a revised SVA/SSP to DHS if your facility updated the Top-Screen and received a revised tier letter that included new chemicals of interest (COI). This revised SVA/SSP should be completed if the new COI is located within a new critical asset, increases the facility's overall tier, creates a new security concern for the facility, or utilizes security measures different than those previously identified in the SVA/SSP. In addition, a facility may need to submit a revised SVA/SSP in order to propose new security measures to DHS, provide clarifying information of current security measures, or correct a previous error.

NOTE After you are notified through CSAT your facility is a Tier 1-4, you have **120 calendar days** to submit an SVA/SSP. When a revised SVA/SSP is necessary, a facility will receive **30 calendar days** to complete the revisions.

What If I Cannot Submit on Time?

A user with a Submitter role can request a due date extension to complete and submit the SVA/SSP survey in the CSAT system.

Upon receipt of the extension request, DHS will review all relevant information and notify your facility of its decision through the CSAT system.

Who Can Fill Out an SVA/SSP?

A Preparer or Submitter can fill out an SVA/SSP. However, only a Submitter will be able to submit an SVA/SSP, once it is complete, to DHS.

NOTE An Authorizer or Reviewer can review the information, but cannot edit it.

Who Can Submit an SVA/SSP?

A Submitter, who is designated by the facility's Authorizer, can submit a SVA/SSP to DHS through the CSAT system in accordance with 6 CFR § 27.200(b)(3).

After the Submitter submits the SVA/SSP, all users assigned to the facility will have access to a PDF version of the survey.

NOTE The Submitter may change/edit the submitted SVA/SSP by using the "Update SVA/SSP" feature in the CSAT Portal. This feature will open a copy of the last submitted SVA/SSP that can be edited. You will have **30 calendar days from the time the** "Update SVA/SSP" is initiated to submit the revised SVA/SSP to DHS. This feature will not be available until after the SVA/SSP is approved. If an edit needs to be done before approval, the submitter may contact their local Chemical Security Inspector for assistance.

What Should I Expect After I Submit My SVA/SSP?

Depending on where your facility is in the CFATS process, various outcomes may occur after the submission of the SVA/SSP survey.

If your facility status is tiered and your facility has not yet been authorized or approved, DHS will review the SVA/SSP to determine whether the SVA/SSP appears to facially satisfy all applicable Risk-Based Performance Standards (RBPS).

If the SVA/SSP does appear to facially satisfy the applicable RBPS, DHS will send your facility a Letter of Authorization. The Authorizer and Submitter will receive an email notification that a new letter is ready for their review and acknowledgement in the CSAT Portal. This letter will initiate the Authorization Inspection process for your facility.

If DHS determines the SVA/SSP does not appear to satisfy the applicable RBPS, DHS will contact your facility to discuss appropriate steps to remedy the apparent deficiencies.

If your facility status is authorized but not approved, DHS will review the SVA/SSP and any Authorization Inspection results and make a final determination as to whether the SVA/SSP satisfies the applicable RBPS.

If the SVA/SSP does satisfy the applicable RBPS, DHS will send your facility a Letter of Approval. The Authorizer and Submitter will receive an email notification that a new letter is ready for their review and acknowledgement in the CSAT Portal. The facility status will change to approved and the facility will be placed in the queue for a Compliance Inspection.

If DHS determines the SVA/SSP does not satisfy the applicable RBPS, DHS will contact your facility to discuss appropriate steps to remedy the apparent deficiencies.

After your facility status is approved, DHS will review any subsequent updates to and/or resubmissions of the SVA/SSP. If the SVA/SSP continues to satisfy the applicable RBPS, DHS will send your facility a new Letter of Approval. The Authorizer and Submitter will receive an email notification that a new letter is ready for their review and acknowledgement in the CSAT Portal. The facility will remain in the queue for a Compliance Inspection.

If DHS determines the SVA/SSP does not satisfy the applicable RBPS, DHS will contact your facility. This could result in a compliance assistance visit or an enforcement action.

If your facility fails to submit an approvable SSP, DHS will attempt to work with the facility to bring the facility into compliance. If a facility fails to come into compliance, DHS has the authority to take appropriate action, including enforcement action, to bring the facility into compliance.

Instructions for Security Vulnerability Assessment (SVA) /Site Security Plan (SSP)

Section references are to the 6 CFR Part 27 Chemical Anti-Terrorism Standards (CFATS) Final Rule unless otherwise noted.

Chemicals of Interest (COIs)

In this section, you will review the high-risk Tier 1-4 chemicals of interest (COI) from your facility's latest tiered Top-Screen. This list will be modified every time a Top-Screen is tiered for your facility.

Tiered COI

Tiered COI are all Tier 1-4 COI that are listed on the facility's latest tiering letter.

NOTE Tiered COIs cannot be removed from the list shown. If your facility no longer possesses a COI listed in this section, or has come into possession of other COI at or above the applicable screening threshold level, you ***MUST*** submit an updated Top-Screen. In addition, you may submit a Top-Screen if your facility plans to possess other COI at or above the applicable screening threshold level.

Q2.10.010 Add Non-Tiered COIs

In this section, the SVA/SSP allows you to voluntarily provide information about non-tiered COI. You may choose to identify these COI and security/vulnerability issues and subsequently provide security measures for these non-tiered COI.

Select the **Add COI** button to identify any COI and associated security/vulnerability issues that DHS has not already identified but that your facility wishes to add to the SVA/SSP.

Otherwise, select **Next**.

NOTE If the non-tiered COI listed is associated with one or more security issues, select all security issues your facility believes to be of concern.

The newly added non-tiered COIs with associated security issues will appear as **Added By User** and you will be required to answer subsequent questions in the SVA/SSP Survey.

NOTE You may reference the CSAT Survey Application User Manual on how to select non-tiered chemicals.

Chemical of Interest (COI) Use

In this section, you are asked to indicate methods of use (i.e., manufacture, sell, ship, and/or receive) of the tiered COIs and all COI added in Question Q2.10.010.

Q2.20.010 Use of COI Tiered and Added by User

Select all the appropriate methods of use displayed for each **Tiered** and **Added by User** COIs, if applicable.

If you select Ship or Receive for a COI, you must also specify **ALL** of the applicable methods used for shipping or receiving the COI (e.g., road, rail, pipeline).

NOTE You must select at least one option for all **Tiered** and/or **Added by User** COIs to proceed to the next question.

Critical Assets

In this section, you are asked to identify the location, name, and description of the critical assets within your facility.

Asset

An asset is any onsite or offsite activities; process(es); systems; subsystems; buildings or infrastructure; rooms; capacities; personnel; or response, containment, mitigation, resiliency, or redundancy capabilities that support the storage, handling, processing, monitoring, inventory/shipping, security, and/or safety of the facility's chemicals, including COI. Assets include but are not limited to:

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

Critical asset

A critical asset is an asset (see definition above) whose theft, diversion, loss, damage, disruption, or degradation would result in a significant adverse impact to human life, national security, or a critical economic asset.

Q2.30.010 Define Critical Assets Present at Facility

In this question, you are asked to define the critical assets at your facility.

Select the **Draw** button from the SVA/SSP drawing tool to begin. The purpose of this question is to use the drawing tool to locate all the critical assets within your facility.

NOTE You may reference the CSAT Survey Application User Manual on how to draw, edit, and delete critical assets with the SVA/SSP drawing tool.

Enter text up to 200 characters to name and describe the critical asset you are reporting. For example, "Name - Northeast Warehouse 1; Description - This warehouse is used to store Phosphine in 15 lb cylinders before being shipped to a customer." The description may also be used to indicate new construction if the imagery is not current.

You will need to describe how you secure these critical assets in your facility's site security plan.

Chemicals of Interest (COI) Association

In this section, you are asked to associate the Tiered (and **Added by User**, if applicable) COI listed in Q2.10.010 to the critical assets listed in Question Q2.20.010. You may have critical assets that do not have any COI associated with them, but each **Tiered** (and **Added by User**, if applicable) COI ***MUST*** be associated with at least one critical asset.

Q2.40.010 Associate COI(s) with Critical Assets

For each critical asset defined in Question Q2.20.010, you will be asked this question.

All COIs must be associated with at least one critical asset to continue with the SVA/SSP survey. You may associate a COI with multiple critical assets.

Vulnerability Assessment

In this section, you are asked to identify different types of measures incorporated to achieve in-depth protection at your facility and its critical assets to mitigate risk.

Q2.50.010 Detection Measures and Identified Vulnerabilities

In this question, you are asked to describe your detection security posture and potential vulnerabilities. Specifically, you are asked to provide a high-level description of the protective measures that are in place to monitor the perimeter and/or critical asset(s) and to detect attacks at early stages. For example, detection security measures may include some combination of (1) personnel or protective force monitoring through stationed positions or roving patrols, (2) intrusion detection systems (IDS), (3) closed circuit television systems (CCTV), (4) lighting, (5) process controls and alarms, and (6) inventory control. After describing the current detection security posture, you should use this information to identify any gaps or vulnerabilities in your posture. For example, potential vulnerabilities may include (1) access points to the perimeter and/or critical asset(s) not currently covered by a method of detection, (2) inoperable or ineffective monitoring system, and (3) lack of training or procedures to support the monitoring capability.

Enter text up to 4,000 characters to describe the measures your facility has in place to detect an attack at early stages and any identified vulnerabilities found while doing this analysis.

Q2.50.020 Delay Measures and Identified Vulnerabilities

In this question, you are asked to describe your delay security posture and potential vulnerabilities. When answering this question consider all delay measures used to secure the perimeter and/or critical asset(s) and afford the facility sufficient time in which to detect an attack prior to the attack becoming successful and allow for appropriate response. For example, delay security measures may include some combination of (1) fencing and walls, (2) vehicle barriers, (3) locking mechanisms, (4) access control, (5) key and credential accountability programs, and (6) screening and inspections. After describing the current delay security posture, you should use this information to identify any gaps or vulnerabilities in your posture. For example, potential vulnerabilities may include (1) access points to the perimeter and/or critical asset(s) lacking an appropriate barrier or locking mechanism, (2) inoperable or ineffective access control system, and (3) lack of training or procedures to support the delay capability.

Enter text up to 4,000 characters to describe the measures your facility has in place to delay an attack for a sufficient period of time and any identified vulnerabilities found while doing this analysis.

Q2.50.030 Response Measures and Identified Vulnerabilities

In this question, you are asked to describe your response capability and potential vulnerabilities. To answer this question, provide information related to developing and exercising an emergency plan within your facility to respond to security incidents internally and with the assistance of local law enforcement and first responders. For example, response security measures may include (1) crisis management plans, (2) elevated and specific threat procedures, (3) communications equipment, (4) outreach with local law enforcement and first responders, (5) security drills and exercises, and (6) release mitigation capabilities. After describing the current response capability, you should use this information to identify any gaps or vulnerabilities in your posture. For example, potential vulnerabilities may include (1) incomplete or lacking documentation, (2) insufficient resources internally or externally, and (3) lack of training or procedures to support the response capability.

Enter text up to 4,000 characters to describe the response measures your facility has taken to enable an appropriate response to an attack and any identified vulnerabilities found while doing this analysis.

Q2.50.040 Cyber Security Measures and Identified Vulnerabilities

In this question, you are asked to describe your cybersecurity measures and potential vulnerabilities. When answering this question, describe the body of technologies, processes, and practices designed to protect critical cyber systems from attack, damage, or unauthorized access. For example, cybersecurity measures may include (1) policies and procedures, (2) access control, (3) password management, (4) personnel security, (5) training and

awareness, (6) cybersecurity controls, monitoring, response and reporting, (7) disaster recovery and business continuity, and (9) system development, maintenance and audit. After describing the current cybersecurity posture, you should use this information to identify any gaps or vulnerabilities in your posture. For example, potential vulnerabilities may include (1) incomplete or lacking documentation, (2) insufficient resources to manage the cybersecurity program, (3) lack of training to support the cybersecurity capability, and (4) access points to the network or system that are not appropriately protected.

Enter text up to 4,000 characters to describe cybersecurity measures and any identified vulnerabilities found while doing this analysis.

Q2.50.050 Policies, Procedures, and Resources and Identified Vulnerabilities

In this question, you are asked to provide measures and vulnerabilities related to the policies, procedures and resources necessary to support the application and management of the facility's security plan and posture. For example, these measures may include (1) inspection, testing, and maintenance program, (2) security awareness and training program, (3) personnel surety, (4) incident reporting and investigations, (5) security organization, and (6) recordkeeping. After describing the current policies, procedures, and resources, you should use this information to identify any gaps or vulnerabilities in your posture. For example, potential vulnerabilities may include (1) incomplete or lacking documentation, (2) insufficient resources to manage the security plan, and (3) lack of training to support the security plan.

Enter text up to 4,000 characters to describe policies, procedures, and resources implemented for the facility's security posture and any identified vulnerabilities found while doing this analysis.

This page is left intentionally blank.

Site Security Plan (SSP) Options

After you complete the COI Association within the SVA survey, you can choose the option that best allows your facility to describe your security measures that satisfy the CFATS RBPS. The options that are available to your facility are based on your facility's tier level. Your tier level is indicated by your facility's latest Top-Screen survey.

Site Security Plan (SSP) Survey

(Available to Tier Levels 1, 2, 3, and 4)

The SSP Survey is a CSAT generated, easy-to-use online questionnaire that allows your facility to describe existing or planned security measures in satisfying the CFATS RBPS.

Alternative Security Program (ASP)

(Available to Tier Levels 1, 2, 3, and 4)

CFATS provides all high-risk facilities with the option of submitting an Alternative Security Program (ASP) in place of the SSP. DHS may approve an ASP, subject to revisions or supplements, if the ASP meets the requirements of 6 CFR § 27.225 and satisfies all applicable RBPS per 6 CFR § 27.230. Revisions or supplements may be made by a facility based on DHS-recommended additional security measures. See 6 USC § 622(c)(2)(A)(iii). Before deciding whether to proceed with this option, your facility should be familiar with the requirements of 6 CFR § 27.225.

See the CSAT Survey Application User Manual for instructions in using the Upload files function.

Expedited Approval Program (EAP)

(Available to Tier Levels 3 and 4)

The CFATS Act of 2014 established an Expedited Approval Program (EAP) as a voluntary option for high-risk chemical facilities assigned a tier level of 3 or 4 to develop and submit SSPs for expedited approval. Facilities utilizing this program must develop their SSP utilizing the prescriptive guidance within the DHS Guidance for the Expedited Approval Program. Along with the EAP SSP, the facility must submit a certification under penalty of perjury that the EAP SSP meets the requirements of 6 USC § 622(c)(4)(C). A sample certification is included in the Guidance.

See the CSAT Survey Application User Manual for instructions in Notifying DHS of EAP, Retract EAP, and Upload files function.

Site Security Plan (SSP) – General

General Considerations

To assist high-risk facilities in selecting a suite of security measures and activities that both meet the CFATS performance standards and are tailored to the unique considerations associated with a facility, DHS offers the following general considerations.

Many RBPS have overlapping requirements and are grouped to most efficiently describe the requirements of the CFATS program. A summary of each RBPS be found in Addendum A. You may reference the RBPS Guidance Document for term definitions and

more details in implementing each RBPS. The SSP survey is organized into overarching security objectives, which collectively account for all of the requirements of the RBPS as described below:

- Detection Measures (RBPS 1, 2, 3, 4, 5, 6, and 7)
- Delay Measures (RBPS 1, 2, 3, 4, 5, 6, and 7)
- Response Measures (RBPS 9, 11, 13, and 14)
- Cyber Security Measures (RBPS 8)
- Security Management Measures (RBPS 7, 10, 11, 12, 15, 16, 17, and 18)

Overarching Security Measures	Risk Based Performance Standards (RBPS) Number																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Detection	✓	✓	✓	✓	✓	✓	✓											
Delay	✓	✓	✓	✓	✓	✓	✓											
Response									✓		✓		✓	✓				
Cyber Security								✓										
Security Management							✓			✓		✓			✓	✓	✓	✓

Table 1: Summary of the SSP Overarching Security Measures and Corresponding RBPS.

Restricted Area

A restricted area means an area where there are special access controls, activity limitations, equipment requirements, or other special, defining measures (usually, but not always, security measures) employed to prevent unauthorized entry; limit access to specific personnel; or elevate security, safety, or some other characteristic to a higher degree of protection.

Asset-Specific vs. Facility-Wide Measures

For many facilities, their level of risk will be driven by a finite number of assets contained within the facility. When this occurs, a facility may want to consider employing asset-specific measures (as opposed to facility-wide measures) to meet the risk associated with the highest risk asset(s). For example, if a ten-acre facility has a single, finite Tier 2 asset and the rest of the assets onsite are Tier 4 risks or not high risk, to implement delay measures, it could be more cost effective for the facility to employ perimeter barriers meeting Tier 2 standards around only the Tier 2 asset, with perimeter barriers meeting Tier 4 standards around the entire facility's perimeter, than it would be to employ perimeter barriers meeting Tier 2 standards around the entire facility.

For many facilities, their level of risk will be influenced by a finite number of assets contained within the facility. When this occurs, a facility may want to consider employing asset-specific measures (as opposed to facility-wide measures) to address the risk associated with the highest risk asset(s) (see CFATS SSP Lessons Learned Tips for Improving Your Submission on the CFATS Knowledge Center, http://csathelp.dhs.gov/). Your facility must clearly identify and describe all COI and critical assets in order to justify taking an asset-based approach versus a facility-wide approach.


You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Detect

In this SSP subsection, you will describe your facility's security plan for its detection measures.

Detection measures are critical to the satisfaction of many of the RBPS and must be applied with overlapping principles of deterrence, delay, and response. Detection refers to the ability to identify potential attacks or precursors to an attack and to communicate that information, as appropriate to personnel responsible for the facility's security. For a protective system to prevail, detection needs to occur prior to an attack (i.e., in the attack-planning stages) or early enough in the attack where there is sufficient delay between the point of detection and the successful conclusion of the attack for the arrival of adequate response forces to thwart the attempt. Therefore, detection and delay are inherently linked. The levels of detection that a facility chooses to implement must be based on the levels of delay implemented and vice versa.

NOTE You may reference Addendum A and the RBPS Guidance Document for more information regarding RBPS requirements and security measures necessary to satisfy the RBPS. The RBPS that satisfy detection measures are: RBPS 1, 2, 3, 4, 5, 6, and 7.

Workforce

In this section you are asked to describe the facility personnel, security personnel, and security force management at your facility.

NOTE If you select **Yes** for Question Q3.10.070, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.010 Security Force

Select **Yes** if your facility maintains onsite security personnel.

Otherwise, select **No**.

*If you select **Yes**, Questions Q3.10.020 - Q3.10.040 will appear. Otherwise, you will skip to Question Q3.10.050.*

Q3.10.020 Security Force Equipment

*If you select **Yes** for Question Q3.10.010, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the security force equipment. Select **No** if your facility does not use the equipment.

Select **Yes** for **Other** if your facility uses any additional security force equipment not listed. If you select this option, you **MUST** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.030 Security Force Weapons

*If you select **Yes** for Question Q3.10.010, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the security force weapon / security device. Select **No** if your facility does not use the device.

Select **Yes** for **Other** if your facility uses any additional security force weapon / security device not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide

clarifying details for any items listed.

Q3.10.040 Onsite Security Force Personnel

*If you select **Yes** for Question Q3.10.010, you **MUST** answer this question.*

This question requires multiple data points in order to complete the answer. Numerical answers must be a positive integer up to 3 digits with no decimal places or commas.

Enter the average number of unarmed security force personnel simultaneously onsite ***AND***;

Enter the total number of unarmed security force personnel employed onsite ***AND***;

Enter the average number of armed security force personnel simultaneously onsite ***AND***;

Enter the total number of armed security force personnel employed onsite ***AND***;

Enter the average response time in minutes for the initial onsite security representative to engage adversaries if an incident occurred at your facility.

Q3.10.050 Personnel Presence

This question requires providing multiple data points in various formats in order to complete the answer.

Select **Yes** if your facility operates 24 hours a day and 7 days a week.

Otherwise, select **No *AND*;**

Enter the minimum number of personnel onsite for ***each time period***. Your answer must be a positive integer up to 6 digits with no decimal places or commas.

NOTE If your facility workforce shifts differ from the time periods listed, provide an estimated average number of personnel on staff for the identified shift periods.

Q3.10.060 Personnel Detection

For each item listed, select **Yes** if your facility utilizes the personnel type at your facility. Select **No** if your facility does not utilize the personnel detection type.

Select **Yes** for **Other** if your facility utilizes any additional personnel types not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.070 Mobile Patrols

For each item listed, select **Yes** if your facility utilizes the mobile patrol type at your facility's perimeter and any identified assets. Select **No** if your facility does not utilize the mobile patrol type.

Select **Yes** for **Other** if your facility utilizes any additional mobile patrol type not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes mobile patrols.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.080 Posted Personnel

Select **Yes** if your facility utilizes posted personnel to provide surveillance of areas and identify unauthorized activities and/or access to materials.

Otherwise, select **No**.

*If you select **Yes,** Question Q3.10.090 will appear. Otherwise, you will skip to Question Q3.10.100.*

Q3.10.090 Posted Personnel Observation

For each item listed, select **Yes** if your posted personnel utilize the observation technique at your facility. Select **No** if your posted personnel do not use the observation technique.

Select **Yes** for **Other** if your facility utilizes any additional observation techniques not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.100 Offsite Security Force Personnel

*If you select **Yes** for Question Q3.10.010 AND Q3.10.080, you **MUST** answer this question.*

This question requires providing multiple data points in various formats in order to complete the answer. Numerical answers above must be a positive integer up to 3 digits with no decimal places or commas.

Enter the estimated average response time for the initial offsite security representative to engage adversaries if an incident occurred at your facility ***AND***;

Enter the estimated average response time for the additional/ backup offsite security representatives to engage adversaries if an incident occurred at your facility ***AND***;

Select **Yes** if these response times are documented and tested in response exercises.

Otherwise, select **No**.

Q3.10.110 Communication Between Management and Workforce

Select **Yes** if your facility ***HAS*** a program to ensure and enhance communication between management and facility personnel to reduce workplace violence and prevent sabotage.

Select **No** if your facility ***DOES NOT HAVE*** a program to ensure and enhance communication between management and facility personnel to reduce workplace violence and prevent sabotage.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Intrusion Detection Systems (IDS)

In this section, you are asked to describe intrusion detection technology and processes utilized within your facility.

NOTE If you select **Yes** for Question Q3.10.120, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.120 Intrusion Detection Systems (IDS)

Select **Yes** if your facility utilizes an IDS.

Otherwise, select **No**.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter are covered by the IDS ***AND***

Questions Q3.10.130 - Q3.10.230 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.

Q3.10.130 Intrusion Detection Systems (IDS) Backup Power Supply

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

Select **Yes**, if your facility's IDS has a backup power supply.

Otherwise, select **No**.

Q3.10.140 Intrusion Detection Systems (IDS) Control

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each location listed, select **Yes** if your facility's IDS can be controlled at the location. Select **No** if your facility does not use the location to control the IDS.

Select **Yes** for **Other** if your facility uses any additional control location for the IDS not listed. If you select this option, you **MUST** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.150 Intrusion Detection Systems (IDS) Administration

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each location listed, select **Yes** if your facility's IDS can be administered at that location. Select **No** if your facility does not use the location for IDS administration.

Select **Yes** for **Other**, if your facility uses any additional administration location for the IDS not listed. If you select this option, you **MUST** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.160 Intrusion Detection Systems (IDS) Monitoring

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each location listed, select **Yes** if your facility's IDS can be monitored at the location. Select **No** if your facility does not use the location for monitoring the IDS.

Select **Yes** for **Other** if your facility uses any additional monitoring location for the IDS not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.170 Intrusion Detection Systems (IDS) Monitoring Frequency

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

Select the **answer** that most accurately describes the monitoring frequency of your facility's IDS.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you **MUST** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Intrusion Detection Sensors (IDS)

In this section, you are asked to describe intrusion detection technology deployed within your facility.

*This section is only available if you select **Yes** for Question Q3.10.120.*

NOTE If you select **Yes** for Questions Q3.10.180, Q3.10.190, Q3.10.200, Q3.10.210, Q3.10.220, and Q3.10.230 you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.180 Fence Mounted Sensors

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your IDS utilizes the type of fence mounted sensor. Select **No** if your IDS does not utilize the sensor type.

Select **Yes** for **Other** if your facility utilizes any additional fence mounted sensor not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes fence mounted sensors.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.190 Volumetric Sensors

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your IDS utilizes the type of volumetric sensor. Select **No** if your IDS ***DOES NOT*** utilize the type of volumetric sensor.

Select **Yes** for **Other** if your facility utilizes any additional volumetric sensors not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes volumetric sensors.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.200 Beam Sensors

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your IDS utilizes this type of beam sensor. Select **No,** if your IDS ***DOES NOT*** utilize this type of beam sensor.

Select **Yes** for **Other**, if your facility utilizes any additional beam sensor not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes beam sensors.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.210 Wall Mounted Sensors

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your IDS utilizes this type of wall mounted sensor. Select **No** if your IDS ***DOES NOT*** utilize this type of wall mounted sensor.

Select **Yes** for **Other** if your facility utilizes any additional wall mounted sensors not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes wall mounted sensors.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.220 Gate/Door Sensors

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your IDS utilizes the type of gate/door sensor. Select **No** if your IDS ***DOES NOT*** utilize the sensor.

Select **Yes** for **Other** if your facility utilizes any additional gate/door sensor not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes gate/door sensors.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.230 Window Mounted Sensors

*If you select **Yes** for Question Q3.10.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your IDS utilizes the type of window mounted sensor. Select **No** if your IDS ***DOES NOT*** utilize the sensor.

Select **Yes** for **Other** if your facility utilizes any additional window mounted sensor not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes window mounted sensors.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Security Lighting

In this section you are asked to describe your facility's security lighting features.

Q3.10.240 Sufficient Illuminations Levels

Select **Yes** if your facility provides sufficient illumination levels for security, safety, and surveillance. ("Sufficient illumination" is lighting that permits individual(s) to perform their duties, provide appropriate surveillance, and properly utilize all security equipment (e.g., CCTV systems).

Otherwise, select **No**.

*If you select **Yes,** Questions Q3.10.250 - Q3.10.260 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.10.250 Security Lighting Backup Power Supply

*If you select **Yes** for Question Q3.10.240, you **MUST** answer this question.*

Select **Yes** if your security lighting has a backup power supply.

Otherwise, select **No**.

Q3.10.260 Lighting in Security Areas

*If you select **Yes** for Question Q3.10.240, you **MUST** answer this question.*

For each item listed, select **Yes** if your lighting system covers the area of your facility. Select **No** if your lighting system ***DOES NOT*** cover the area.

Select **Yes** for **Other**, if your lighting system covers any additional areas of your facility not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

*If you select **Yes for Security gates lighting**, Question Q3.10.270 will appear. If you select **Yes for Critical assets lighting**, Question Q3.10.280 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.10.270 Security Gates Covered by Security Lighting

*If you select **Yes for Security gates lighting** for Question Q3.10.260, you **MUST** answer this question.*

Enter a numerical value representing the percentage of security gates covered by security lighting. The value may have up to two decimal places and cannot be greater than 100%. For example, if lighting covers 75.75% of your facility security gates, enter 75.75.

Q3.10.280 Critical Assets Covered by Security Lighting

*If you select **Yes for Critical assets lighting** for Question Q3.10.260, you **MUST** answer this question.*

Enter a numerical value representing the percentage of critical assets covered by security lighting. The value may have up to two decimal places and cannot be greater than 100%. For example, if lighting covers 75.75% of your facility critical assets enters 75.75.

Closed Circuit Television (CCTV)

In this section you are asked to describe CCTV utilized within your facility.

NOTE If you select **Yes** for Questions Q3.10.290 and Q3.10.310, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.290 Closed Circuit Television (CCTV)

Select **Yes**, if your facility utilizes a CCTV system.

Otherwise, select **No**.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes CCTV systems.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

*If you select **Yes,** Questions Q3.10.300 - Q3.10.380 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.10.300 CCTV System Backup Power Supply

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

Select **Yes** if your CCTV system has a backup power supply.

Otherwise, select **No**.

Q3.10.310 CCTV Coverage Area

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

For each location listed, select **Yes** if your CCTV system covers the area within your facility. Select **No** if your CCTV system *DOES NOT* cover this area of your facility.

Select **Yes** for **Other** if your CCTV system covers any additional areas of your facility not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for this question, you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter are covered by CCTV.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.10.320 CCTV Integration with Access Control System

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

Select **Yes** if your CCTV system is integrated with your access control system (ACS).

Otherwise, select **No**.

Q3.10.330 CCTV Integration with Intrusion Detection System

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

Select **Yes**, if your CCTV system is integrated with your intrusion detection system.

Otherwise, select **No**.

Q3.10.340 CCTV System Control

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

For each location listed, select **Yes** if your CCTV system can be controlled at the location. Select **No** if your CCTV system *cannot* be controlled in the location.

Select **Yes** for **Other** if your facility utilizes any additional CCTV system control location not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.350 CCTV System Administration

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

For each item location, select **Yes** if your CCTV system can be administered at the location. Select **No** if your CCTV system *cannot* be administered in the location.

Select **Yes** for **Other** if your facility utilizes any additional CCTV system administration location not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.360 CCTV System Monitoring

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

For each location listed, select **Yes** if your CCTV system can be monitored at the location. Select **No** if your CCTV system *cannot* be monitored in the location.

Select **Yes** for **Other** if your facility utilizes any additional CCTV system monitoring methods not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.370 CCTV System Staffing and Monitoring

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

Select the **answer that best describes** your facility's CCTV system staffing and monitoring.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.10.380 CCTV Facility Coverage

*If you select **Yes** for Question Q3.10.290, you **MUST** answer this question.*

This question requires multiple data points in order to complete the answer.

Enter a numerical value to describe the percentage of your facility's CCTV coverage:

- Perimeter fencing ***AND*;**
- Gates monitored ***AND*;**
- Critical locations (critical assets, loading/unloading areas, storage vessels, etc.).

All answers above must be a positive value up to one decimal place and cannot be greater than 100%. For example, if CCTV covers 75.75% of your facility gates, enter 75.8.

Process Controls

In this section you are asked to describe process control functions supporting your facility's detection measures.

Q3.10.390 Process Controls

Select the **answer** that most accurately describes your facility's process control functions.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Inventory Controls

In this section you are asked to describe inventory control processes utilized within your facility.

Q3.10.400 Inventory Controls

Select **Yes** if your facility has written procedures for inventory control.

Otherwise, select **No**.

Q3.10.410 Inventory Control Records

Select **Yes** if your facility maintains inventory records.

Otherwise, select **No**.

Q3.10.420 Formal Inventory

Select the **frequency that best describes** your facility's formal inventory of its COI(s).

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed and to describe informal inventory control measures.

Detection - Planned Measures

In this section, you are asked to describe planned security measures that enhance your facility's detection measures.

A planned security measure may be considered by DHS in determining whether an SSP satisfies an applicable RBPS, for example, if the measure:

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

If a facility chooses to provide information about a planned security measure for consideration, DHS may subsequently ask the facility to produce documentation confirming the planned measure.

Upon approval of your SVA/SSP survey, planned measures may become enforceable components of that facility's final SSP.

Q3.10.430 Planned Measures

Enter up to 4,000 characters in the text box to describe any planned security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS. You ***MUST*** identify the number of months, not to exceed 36 months, within which your facility intends to implement the planned measure after you receive approval of the SSP from DHS. This timeframe should be reasonable and commensurate to the planned action taking place.

Detection - Proposed Measures

In this section, you are asked to describe any proposed security measures that enhance your facility's detection measures.

You can provide three types of information for proposed measures:

(1) Proposed Security Measures your facility wants to share with DHS;

(2) Existing Security Measures your facility is proposing to eliminate or remove; and

(3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

You may reference Addendum B for more information for entering proposed security measures.

Q3.10.440 Proposed Measures

Enter up to 4,000 characters in the text box to describe any proposed security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS.

Proposed security measures ***ARE NOT*** considered as part of formal evaluation of your facility's SSP; however, DHS may provide feedback to facilities on the proposed measures listed if they would assist the facility in satisfying a particular RBPS.

Delay

In this section you will describe your facility's security plan for its delay measures.

Delay means physically limiting the accessibility of the facility or critical asset(s) such that there is a low likelihood of an adversary successfully breaching the facility perimeter or critical asset(s) or using the area immediately outside of the facility's perimeter to launch an attack. Completely adequate perimeter security is rarely achievable through the deployment of a single security barrier; rather an optimal security solution typically involves the use of multiple protective measures providing layers of security. Layering of security measures can be achieved in many different manners, such as incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems, with procedural security measures, such as procedures guiding how security personnel should respond to an incident). A layered approach to perimeter security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

You may reference RBPS 1, 2, 3, 4, 5, 6, and 7 in Addendum A and the RBPS Guidance Document for further information regarding RBPS requirements and security measures necessary to satisfy the RBPS.

Perimeter Security

In this section, you are asked to describe your facility's system used to secure the perimeter to delay or restrict attempts by unauthorized persons to gain access to the facility.

NOTE If you select **Yes** or **Other**, for Questions Q3.20.030, Q3.20.070, Q3.20.080, Q3.20.090, Q3.20.110, Q3.20.120, Q3.02.140, Q3.20.150, and Q3.20.160 you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.010 Defined Perimeter

Select **Yes** if your facility has a defined perimeter marked by company property, has no trespassing signage, fencing, or other barriers.

Select **Partial** if your facility has some of the facility perimeter defined.

Otherwise, select **No**.

You can use the "Additional Information" text box to provide clarifying details.

*If you select **Yes** or **Partial,** Question Q3.20.020 will appear. Otherwise, you will skip to Question Q3.20.030.*

Q3.20.020 Defined Perimeter Characteristics

*If you select **Yes** or **Partial** in Question Q3.20.010, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the measure to define its perimeter. Select No if your facility does not use the perimeter characteristic.

Select **Yes** for **Other** if your facility uses any additional perimeter characteristics not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.030 Standoff Distance

Select **Yes** if your facility maintains standoff distance. **Standoff distance** is a security measure that focuses on preventing unscreened people and vehicles from approaching within a certain distance of the facility perimeter or a critical asset. Otherwise, select **No**.

You can use the "Additional Information" text box to provide clarifying details for the facility's standoff distance.

If you select **Yes** for this question you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter have a defined standoff distance.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.040 Topographical Barriers

For each item listed, select **Yes** if your facility has the topographical barrier. Select **No** if your facility does not have the barrier.

Select **Yes** for **Other** if your facility uses any additional topographical barrier not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.050 Landscaping Barriers

For each item listed, select **Yes** if your facility has the landscaping barrier. Select **No** if your facility does not have the barrier.

Select **Yes** for **Other** if your facility uses any additional landscaping barrier(s) not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.060 Vegetation

Select the answer that most accurately describes your facility.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for the control program for clear zones and perimeter barriers present in your facility.

For example, *a clear zone* (i.e., zones that are not subject to environmental disturbances, such as foliage, birds, squirrels, etc.) can be present on either side of the facility's fence that allows persons to be detected at the boundary.

Q3.20.070 Fence

For each item listed, select **Yes** if your facility uses the fence barrier. Select **No** if your facility does not use the barrier.

Select **Yes** for **Other** if your facility uses any additional fence barrier not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the fence barrier listed.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.080 Fence Top Guard

For each item listed, select **Yes** if your facility uses the fence top guard. Select **No** if your facility does not use the top guard.

Select **Yes** for **Other** if your facility uses any additional fence top guard not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the fence top guard listed.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.090 Wall

For each item listed, select **Yes** if your facility uses the wall type. Select **No** if your facility does not use the wall type.

Select **Yes** for **Other** if your facility uses any additional wall type not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the wall type listed.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.100 Gate

Select **Yes** if your facility perimeter barrier and/or critical asset(s) have any gates.

Otherwise, select **No**.

*If you select **Yes,** Questions Q3.20.110 - Q3.20.120 will appear. Otherwise, you will skip to Question Q3.20.130.*

Q3.20.110 Gate Material

*If you select **Yes** in Question Q3.20.100, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the gate material. Select **No** if your facility does not use the material.

Select **Yes** for **Other** if your facility uses any additional gate material not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the gate material listed.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.120 Gate Hardware

*If you select **Yes** in Question Q3.20.100, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the gate hardware. Select **No** if your facility does not use the hardware.

Select **Yes** for **Other** if your facility uses any additional gate hardware not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the gate hardware listed.

NOTE You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.130 Door

Select **Yes** if your facility perimeter barrier and/or critical asset(s) have any doors.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.20.140 - Q3.20.150 will appear. Otherwise, you will skip to Question Q3.20.160.*

Q3.20.140 Door Material

*If you select **Yes** in Question Q3.20.130, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the door material. Select **No** if your facility does not use the material.

Select **Yes** for **Other** if your facility uses any additional door material not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the door material listed.

Q3.20.150 Door Hardware

*If you select **Yes** in Question Q3.20.130, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the door hardware. Select **No** if your facility does not use the hardware.

Select **Yes** for **Other** if your facility uses any additional door hardware not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the door hardware listed.

Q3.20.160 Anti-Personnel Barrier

For each item listed, select **Yes** if your facility uses the anti-personnel barrier. Select **No** if your facility does not use the barrier.

Select **Yes** for **Other** if your facility uses any additional door hardware not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the anti-personnel barrier listed.

Q3.20.170 Access Points

For each item listed, select **Yes** if your facility has the type of access point. Select **No** if your facility does not have the access point.

Select **Yes** for **Other** if your facility uses any additional access point not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Secure Site Assets

In this section, you are asked to describe the measures your facility uses to secure restricted areas and/or critical assets.

In the context of securing site assets, "secure" means physically limiting the accessibility of the asset to reduce the likelihood of unauthorized release, theft, or sabotage. Securing an asset is frequently accomplished by using a combination of one or more layers of physical barriers (e.g., fencing, man-made obstacles, natural obstacles) and guard forces.

Q3.20.180 Restricted / Secure Areas

Select **Yes** if your facility defines restricted or secure areas for critical assets within its perimeter barrier.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.20.190 - Q3.20.220 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.20.190 Screening for Restricted Area Access

*If you select **Yes** in Question Q3.20.180, you **MUST** answer this question.*

Select the answer that most accurately describes your facility's screening measures for accessing its restricted areas.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for the control program for clear zones and perimeter barriers present in your facility.

Q3.20.200 Restricted Areas

*If you select **Yes** in Question Q3.20.180, you **MUST** answer this question.*

For each item listed, select **Yes** if the statement describes your facility's restricted areas. Select **No** if the statement does not describe your facility.

Select **Yes** for **Other** if statements regarding your facility's restricted area are not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.210 2-Person Rule

*If you select **Yes** in Question Q3.20.180, you **MUST** answer this question.*

The two-person rule is a control mechanism designed to achieve a high level of security critical asset(s) or restricted areas. Under this rule all access and actions requires the presence of two authorized people at all times.

Select **Yes** if your facility defines restricted or secure areas for critical assets within its perimeter barrier and employs the 2-person rule for such areas and assets.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.220 Internal Barriers

*If you select **Yes** in Question Q3.20.180, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the barrier classification securing site assets. Select **No** if your facility does not use the barrier.

Select **Yes** for **Other** if your facility uses any additional internal barrier not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Screening and Access Control

In this section, you are asked to describe your facility's screening program element which includes any vehicle identification and vehicle or hand-carried item inspection program. Vehicle identification measures can include using a company- or facility-issued vehicle ID system (e.g., providing authorized vehicles with stickers or placards), using only known shippers and/or delivery companies, and requiring authorized bills of lading for access to the facility.

Vehicle and hand-carried item inspection measures that can be helpful in meeting the screening and access control standards include:

- Visual inspections,
- Use of trained explosives detection canines,
- Under/over vehicle inspection systems, and
- Cargo inspection systems.

The type of inspection measures implemented, the thoroughness of inspections, and the frequency of inspections may vary on the basis of a variety of factors, including the facility's tier (e.g., more vigorous and frequent inspections may be suitable for higher tiers) and what is being inspected (e.g., more frequent and thorough inspections may be desired for visitors or unscheduled delivery trucks than for employees or regularly scheduled deliveries).

Q3.20.230 Screening for Facility Areas

Select the answer **that best describes your facility's** overall screening of personnel and vehicles entering the facility.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for the screening program for facility access.

Q3.20.240 Vehicle Inspection

Select **Yes** if your facility inspects vehicles seeking to access your facility.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.20.250 - Q3.20.270 will appear. Otherwise, you will skip to Question Q3.20.280.*

Q3.20.250 Inspection Methods

*If you select **Yes** in Question Q3.20.240, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the inspection method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional inspection method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.260 Inbound Vehicle Inspection Methods

*If you select **Yes** in Question Q3.20.240, you **MUST** answer this question.*

For each item listed:

Select **Not Allowed on site** if your facility does not allow the vehicle type to enter the facility.

Select **Inspection of all vehicles** if your facility inspects all the vehicles of the listed type prior to entering the facility.

Select **Inspection of a percentage of vehicles** if your facility performs random inbound vehicle inspections of the vehicle type listed. If you select this option, you ***MUST*** also provide a **percentage value.**

Select **Not applicable** if your facility does not have the vehicle type seeking access to the facility.

Q3.20.270 Inbound Truck and Railcar Inspection Methods

*If you select **Yes** in Question Q3.20.240, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the inspection method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional inspection method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.280 Inbound Hand Carried Item Inspections

Select **Yes** if your facility inspects items hand carried by individuals seeking access to the facility.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.20.290 will appear. Otherwise, you will skip to Question Q3.20.300.*

Q3.20.290 Inbound Hand Carried Item Inspection Methods

*If you select **Yes** in Question Q3.20.280, you **MUST** answer this question.*

For each type of inbound personnel listed, select **the inspection range value** your facility uses to inspect inbound hand carried items.

Q3.20.300 Vehicle Access into Restricted Areas Containing Theft COI

Select **Yes** if vehicles are allowed access into restricted areas containing Theft Chemical of Interest (COI).

Otherwise, select **No.**

*If you select **Yes,** Question Q3.20.310 will appear. Otherwise, you will skip to Question Q3.20.330.*

DHS identifies the following as Theft/Diversion COI:

(A) Explosives (EXP)/Improvised Explosive Device Precursors (IEDP) COI as those that could be stolen or diverted and used as explosives or within Improvised Explosive Devices (IEDs).

(B) Weapons of mass effect (WME) COI as those that could be stolen or diverted and used directly as WME.

(C) Chemical Weapons (CW)/Chemical Weapons Precursor (CWP) COI as those that could be stolen or diverted and used as CW or easily converted into CW.

Q3.20.310 Outbound Vehicle Inspections

*If you select **Yes** in Question Q3.20.300, you **MUST** answer this question.*

Select **Yes** if your facility inspects outbound vehicles from restricted areas containing Theft COI.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.20.320 will appear. Otherwise, you will skip to Question Q3.20.330.*

Q3.20.320 Outbound Vehicle Inspection Methods

*If you select **Yes** in Q3.20.310, you **MUST** answer this question.*

For each item listed: Select **Not Allowed on site** if your facility does not allow the outbound vehicle type to enter the facility's restricted area. Select **Inspection of all vehicles** if your facility inspects all the vehicles of the listed type prior to exiting the facility's restricted area. Select **Inspection of a percentage of vehicles** if your facility performs random outbound vehicle inspections of the vehicle type listed. If you select this option, you ***MUST*** also provide a **percentage value.**

Select **Not applicable** if your facility does not allow vehicles into the facility.

Q3.20.330 Inspection of Outbound Hand Carried Items

Select **Yes** if your facility inspects items hand carried by individuals leaving restricted areas that contain Theft COI.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.20.340 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.20.340 Outbound Hand Carried Item Inspection

*If you select **Yes** in Q3.20.330, you **MUST** answer this question.*

For each type of inbound personnel listed, select **the inspection range value** your facility uses to inspect outbound hand carried items.

Personnel Access

In this section, you are asked to describe your facility's practice of restricting entrance to the facility and/or critical assets to authorized persons.

Q3.20.350 Identification Verification System

For each item listed, select **Yes** if your facility uses the identification verification method. Select **No** if your facility does not use the method to verify the identity of individuals at the facility.

Select **Yes** for **Other** if your facility uses any additional identification verification method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.360 Personnel Access Control

For each item listed, select **Yes** if your facility personnel uses the method to control access to the facility. Select **No** if your facility does not use the access control.

Select **Yes** for **Other** if your facility uses any additional access control not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.370 Badges

Select **Yes** if your facility personnel, contractors, and/or visitors are required to have badges.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.20.380 - Q3.20.410 will appear. Otherwise, you will skip to Question Q3.20.420.*

Q3.20.380 Control Measures

*If you select **Yes** in Question Q3.20.370, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the control measure. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional control measure not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.390 Photo Badge Usage

*If you select **Yes** in Question Q3.20.370, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the photo badge method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional photo badge method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.400 Non-Photo Badge Usage

*If you select **Yes** in Question Q3.20.370, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the non-photo badge method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional non-photo badge method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.410 Types of Badges Used at Facility

*If you select **Yes** in Question Q3.20.370, you **MUST** answer this question.*

For each badge type listed, select **Yes** if your facility personnel, contractors or visitors use the badge type. Select **No** if your facility personnel, contractors or visitors do not use the badge type. Select **Not Applicable (N/A)** if your facility does not use the badge type.

Q3.20.420 Visitor Access

For each item listed, select **Yes** if your facility uses the escort policy. Select **No** if your facility does not use the policy.

Select **Yes** for **Other** if your facility uses any additional escort policy not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Access Control System

In this section, you are asked to describe your facility's electronic access control system, if applicable. Electronic access control systems can be tailored to specific locations within a facility, thus providing the ability to limit access to restricted areas to authorized individuals. They also have the additional benefit of maintaining a record regarding who has accessed what areas.

NOTE If you select **Yes**, for Questions Q3.20.430 and Q3.20.440 you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.430 Access Control System

Select **Yes** if your facility has an access control system (ACS).

Otherwise, select **No.**

NOTE If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use an ACS. You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

*If you select **Yes,** Questions Q3.20.440 - Q3.20.480 will appear. Otherwise, you will are finished with this subsection.*

Q3.20.440 Access Control System

*If you select **Yes** in Question Q3.20.430, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the Access Control System (ACS) interface. Select **No** if your facility does not use the interface.

Select **Yes** for **Other** if your facility uses any additional ACS interface not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the ACS interface listed.

You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.450 ACS Control

*If you select **Yes** in Q3.20.430, you **MUST** answer this question.*

For each location listed, select **Yes** if your facility's ACS can be controlled at the location. Select **No** if your facility does not use the location to control the ACS.

Select **Yes** for **Other** if your facility uses any additional control location for the ACS not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.460 ACS Administration

*If you select **Yes** in Question Q3.20.430, you **MUST** answer this question.*

For each location listed, select **Yes** if your facility's ACS can be administered at the location. Select **No** if your facility does not use the location for ACS administration.

Select **Yes** for **Other** if your facility uses any additional administration location for the ACS not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.470 ACS Monitoring

*If you select **Yes** in Question Q3.20.430, you **MUST** answer this question.*

For each location listed, select **Yes** if your facility's ACS can be monitored at the location. Select **No** if your facility does not use the location for monitoring the ACS.

Select **Yes** for **Other** if your facility uses any additional monitoring location for the ACS not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.480 ACS Backup Power Supply

*If you select **Yes** in Question Q3.20.430, you **MUST** answer this question.*

Select **Yes** if your facility has backup power supply for its ACS.

Otherwise, select **No.**

Vehicle Restrictions

In this section, you are asked to describe your facility's practice of restricting entrance to the facility and/or critical assets to authorized vehicles.

NOTE If you select **Yes**, for Question Q3.20.560 you ***MUST*** indicate which of your facility's critical asset(s) and/or facility perimeter utilizes the measure in question.

You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.490 Vehicle Access Restrictions

For each item listed, select **Yes** if your facility uses the vehicle restriction method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional vehicle restriction method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.500 Vehicle Identification

For each item listed, select **Yes** if your facility uses the vehicle identification method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional vehicle identification method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.510 Traffic Calming/Speed Reduction Measures

For each item listed, select **Yes** if your facility uses the traffic calming /speed reduction control measure. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional speed reduction control measure not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.520 Employee Parking Restrictions

For each item listed, select **Yes** if your facility uses the employee parking restriction. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional employee parking restriction not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.530 Contractor Parking Restrictions

For each item listed, select **Yes** if your facility uses the contractor parking restriction. Select **No** if your facility does not use the restriction.

Select **Yes** for **Other** if your facility uses any additional contractor parking restriction not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.540 Delivery Parking Restrictions

For each item listed, select **Yes** if your facility uses the delivery parking restriction. Select **No** if your facility does

not use the restriction.

Select **Yes** for **Other** if your facility uses any additional delivery parking restriction not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.550 Visitor Parking Restrictions

For each item listed, select **Yes** if your facility uses the visitor parking restriction. Select **No** if your facility does not use the restriction.

Select **Yes** for **Other** if your facility uses any additional visitor parking restriction not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.560 Anti-Vehicle Measures

For each item listed, select **Yes** if your facility uses the anti-vehicle measure. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional anti-vehicle measure not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

If you select **Yes** for an item you **MUST** indicate which of your facility's critical asset(s) and/or facility perimeter barrier use the anti-vehicle measure listed.

You can modify your facility's critical assets at any time prior to submitting your SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Q3.20.570 Anti-Vehicle Measure Backup Power

Select **Yes** if your facility has backup power supply for any anti-vehicle measures identified in Question Q3.20.570. This applies only to those measures where backup power would be applicable.

Otherwise, select **No.**

Key and Credential Inventory / Control Program

In this section, you are asked to describe your facility's procedures, inventory control systems and/or physical measures that can monitor and/or track the keys, credentials, locks, combinations and codes that grant access to the facility.

Q3.20.590 Key Inventory/Control Program

Select **Yes** if your facility ***HAS*** a program managing key/lock, combination, and access credential control and accountability.

Select **No** if your facility ***DOES NOT HAVE*** a program managing key/lock, combination, and access credential control and accountability.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

*If you select **Yes,** Questions Q3.20.600 - Q3.20.630 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.20.600 Key Inventory/Controls

*If you select **Yes** in Question Q3.20.590, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the key inventory measure. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional key inventory measure not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.610 Key and Credential Controls

*If you select **Yes** in Question Q3.20.590, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the key control security measure. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional key control measure not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.620 Key and Credential Compromise

*If you select **Yes** in Question Q3.20.590, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility follows the key compromise procedure. Select **No** if your facility does not follow the procedure.

Select **Yes** for **Other** if your facility uses any additional key compromise procedure not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.630 Key and Credential Inventory

*If you select **Yes** in Question Q3.20.590, you **MUST** answer this question.*

This question requires answering multiple data points.

Enter the frequency in weeks which your facility conducts inventory for the following:

- **Keys *AND*;**
- **Locks *AND*;**
- **Key and Lock Combinations *AND*;**
- **Access Credentials.**

The answer must be a positive integer up to 5 digits with no commas or period. For example if your facility conducts inventory annually, enter the number 52.

Shipping, Receiving, and Storage

In this section, you are asked to describe the procedures and measures used to secure and monitor the shipping, receipt, and storage of chemicals of interest tiered for the facility.

Improved inventory control and control of transportation containers on-site helps to prevent tampering or sabotage, and decreases the likelihood of theft, diversion, or a foreign substance being introduced into feedstock, incidental chemicals, or products that are leaving the facility and that could later interact with the hazardous material to cause a harmful reaction on- or off-site. Good shipping, receipt, and storage practices typically include maintaining all containers that are used for storage but are not incident to transportation, including transportation containers connected to equipment at a facility for loading or unloading and transportation containers detached from the motive power (e.g., a locomotive, truck/tractor) that delivered the container to the facility, inside the facility's security perimeter and under the security control of the facility.

Q3.20.640 Know Your Customer

An active, documented "know your customer" program includes a policy of refusing to sell hazardous materials to those who do not meet the pre-established customer qualification criteria. Examples of such criteria may include:

- Verification and/or evaluation of the customer's on-site security,
- Verification that shipping addresses are valid business locations,
- Confirmation of financial status,
- Establishment of normal business-to-business payment terms and methods (e.g., not allowing cash sales), and
- Verification of product end-use.

Select **Yes** if your facility ***HAS*** a "know your customer" program.

Select **No** if your facility ***DOES NOT*** have a "know your customer" program.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.20.650 Product Stewardship Program

Product stewardship is a term used to describe a product-centered approach to protection of hazardous materials, and calls for manufacturers, retailers, and consumers to share responsibility for reducing the potential for theft, contamination, or misuse of chemicals.

Select **Yes** if your facility ***HAS*** a product stewardship program.

Select **No** if your facility ***DOES NOT*** **have** a product stewardship program.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.20.660 Documentation of Sales and Purchases to or from Manufacturers

Select **All** if your facility documents ***ALL*** sale and purchase of COI to/from manufacturers and distribution of COI.

Select **Most** if your facility documents ***SOME BUT NOT ALL*** sales and purchases of COI to/from manufacturers and distribution of COI.

Select **None** if your facility ***DOES NOT*** document any sale and purchase of COI to/from manufacturers and distribution of COI.

Q3.20.670 Documentation of Sales and Purchases to or from Third Parties

Select **All** if your facility documents ***EVERY*** sale and purchase of COI to/from third parties and distribution of COI.

Select **Most** if your facility documents ***SOME BUT NOT ALL*** sales and purchases of COI to/from third parties and distribution of COI.

Select **None** if your facility ***DOES NOT*** document any sale and purchase of COI to/from third parties and distribution of COI.

Q3.20.680 Cross-Referenced and Real-Time Review of Transactions

Select **Yes** if your facility cross-references and provides real-time review of transactions for the sales and distribution of COI.

Otherwise, select **No.**

Q3.20.690 Duplicate Review and Validation of Shipping, Receiving and Delivery Documents

Select **Yes** if your facility has a procedure in place to ensure duplicate review and validation of shipping, receiving, and delivery documents for COI.

Otherwise, select **No.**

Q3.20.695 Shipping, Receiving and Storage Documentation Additional Information

Enter text up to 4,000 characters to provide any additional information for questions Q3.20.660 - Q3.20.690.

Q3.20.700 Confirmation of Shipments for On-site Driver/Passengers

Select **All** if your facility confirms ***EVERY*** shipment before allowing the driver/passengers on-site.

Select **Most** if your facility confirms ***SOME BUT NOT ALL*** shipments before allowing the driver/passengers on-site.

Select **None** if your facility ***DOES NOT*** confirm the shipments before allowing the driver/passengers on-site.

Q3.20.710 Advanced Planning and Approval of Inbound and Outbound Shipments

What number of inbound and outbound shipments of COI does the facility conduct advanced planning and approval of?

Select **All** if your facility conducts advanced planning and approval for ***EVERY*** inbound and outbound shipments of COI.

Select **Most** if your facility conducts advanced planning and approval for ***SOME BUT NOT ALL*** inbound and outbound shipments of COI.

Select **None** if your facility ***DOES NOT*** conduct advanced planning and approval for inbound and outbound shipments of COI.

Q3.20.720 ID Checks for Customer Pickup of COI

Select **Yes** if your facility ***DOES*** conduct proper identification checks and verifications prior to customer pickup of COI.

Select **No** if your facility ***DOES NOT*** conduct proper identification checks and verifications prior to customer pickup of COI.

Select **Not Applicable** if your facility ***DOES NOT HAVE*** customer pickup.

Q3.20.730 Planning and Approving of Shipments by Approved Carriers

Select **Yes** if your facility plans and approves all shipments in advance using known, approved carriers.

Otherwise, select **No.**

Q3.20.740 Security Measures by Approved Carriers

Select **Yes** if your facility's approved carriers implemented security measures to provide protection of the vehicle and materials being transported by them.

Otherwise, select **No.**

Q3.20.750 Security Surveys by Carriers

Select **Yes** if your facility's carriers conduct security surveys to ensure compliance and effectiveness of security and protection measures.

Otherwise, select **No.**

Q3.20.760 En Route Material Storage

Select **Yes** if your facility stores material in transit in secure facilities.

Otherwise, select **No.**

Q3.20.770 Tracking Shipments En Route

Select **Yes** if your facility has systems in place to track or protect shipments in transit to their destinations, such as drive call-in schedules, GPS tracking, etc.

Otherwise, select **No.**

Q3.20.775 Carrier Additional Information

Enter text up to 4,000 characters to provide any additional information for questions Q3.20.730 - Q3.20.770.

Q3.20.780 Additional Protections for Man-Portable Containers

Select **All** if your facility identified and provided additional protection, such as being chained and locked or otherwise affixed to larger immobile objects or special security tie-downs for ***EVERY*** man-portable container containing COI within the facility.

Select **Most** if your facility identified and provided additional protection, such as being chained and locked or otherwise affixed to larger immobile objects or special security tie-downs for ***SOME BUT NOT ALL*** man-portable container containing COI within the facility.

Select **None** if your facility ***DOES NOT*** provide additional protection for man-portable container containing COI within the facility.

*If you select **Yes,** Question Q3.20.790 will appear. Otherwise, you will skip to Question Q3.20.800.*

Q3.20.790 Security Measures of Man-Portable Containers

*If you select **Yes** in Question Q3.20.780, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the security measure. Select **No** if your facility does not use the measure.

Select **Yes** for **Other** if your facility uses any additional key security measure for man-portable containers containing COI not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.800 Procedures for Controlling Activities Related to Purchase and Sale

For each item listed, select **Yes** if your facility has procedures in place related to the purchase and sale of hazardous materials (including COI). Select **No** if your facility does not have the procedure in place.

Select **Yes** for **Other** if your facility uses any additional procedures to control activities related to the purchase and sale of hazardous materials not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.810 Monitoring Features for Storage of Hazardous Materials

For each item listed, select **Yes** if your facility has monitoring features in place to monitor hazardous materials (including COI) stored at the facility. Select **No** if your facility does not have the monitoring feature in place.

Select **Yes** for **Other** if your facility uses any additional monitoring feature not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.820 Monitoring of Shipping and Receiving Areas

Select **Yes** if your facility has holding areas for carriers awaiting loads or staged for unloading are secured when vehicles/area is unattended.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details.

Q3.20.830 Vehicle Inspections

Select **Yes** if your facility provides secure vaults within vehicle(s), and issues tanker truck keys only to authorized drivers.

Otherwise, select **No.**

Q3.20.840 Tamper-Evident Devices

Select **Yes** if your facility has a system for identifying and reporting evidence of tampering with COI.

Otherwise, select **No.**

Q3.20.850 Tamper-Evident Mechanisms

For each item listed, select **Yes** if your facility uses tamper-evident mechanisms to identify tampering with hazardous materials (including COI). Select **No** if your facility does not use the tamper evident mechanism. Select **Not Applicable** if the item listed does not apply to your facility.

Select **Yes** for **Other** if your facility uses any additional the tamper evident mechanism not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You **can** use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.860 Tamper-Evident Seals for Vehicle Valves

Select **Yes** if your facility employs tamper-evident seals for vehicle valves to indicate if a shipment has been tampered with.

Otherwise, select **No.**

Q3.20.870 Tamper-Evident Seals for Other Equipment

Select **Yes** if your facility employs tamper-evident seals for accessories or equipment that can indicate if there is evidence of tampering on a shipment.

Otherwise, select **No.**

Q3.20.880 Controls for Preventing Theft of Hazardous Materials

For each item listed, select **Yes** if your facility has the control measure to prevent the theft of hazardous materials (including COI). Select **No** if your facility does not have the theft prevention control in place.

Select **Yes** for **Other** if your facility uses any theft prevention control not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.890 Maximizing Transportation Security

For each item listed, select **Yes** if your facility uses the method to maximize transportation security. Select **No** if your facility does not use the tamper evident method.

Select **Yes** for **Other** if your facility uses any additional the transport security method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You **can** use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.20.900 Rail/Tanker Storage

Check **the answers that best describe** your facility's rail/tanker storage measures to prevent sabotage. You may select more than one answer.

Select **Other** if you have additional rail/tanker storage measures to prevent sabotage. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Delay - Planned Measures

In this section, you are asked to describe planned security measures that enhance your facility's delay measures.

A planned security measure may be considered by DHS in determining whether an SSP satisfies an applicable RBPS, for example, if the measure:

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

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

Upon submitting your SVA/SSP survey these may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. Of course, if your facility chooses not to provide information about an existing or planned measure that is relevant to the satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Q3.20.910 Planned Measures

Enter up to 4,000 characters in the text box to describe any planned security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS. You ***MUST*** identify the number of months within which your facility intends to implement the planned measure, not to exceed 36 months, after you receive approval of the SSP from DHS. This timeframe should be reasonable and commensurate to the planned action taking place.

Only existing and planned security measures are considered in the formal evaluation of your facility's submitted SSP. Proposed measures will not be considered in the formal evaluation of your facility's submitted SSP.

Delay - Proposed Measures

In this section, you are asked to describe any proposed security measures that enhance your facility's delay measures.

You can provide three types of information for proposed measures:

(1) Proposed Security Measures your facility wants to share with DHS;

(2) Existing Security Measures your facility is proposing to eliminate or remove; and

(3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

You may reference Addendum B for more information for entering proposed security measures.

Q3.20.920 Proposed Measures

Enter up to 4,000 characters in the text box to describe any proposed security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS.

Proposed security measures ***ARE NOT*** considered as part of formal evaluation of your facility's SSP; however, DHS may provide feedback to facilities on the proposed measures listed if they would assist the facility in satisfying a particular RBPS.

Response

Response within the security plan context primarily refers to the response of appropriately trained personnel (either facility personnel or external first responders) to a threat or actual theft or release of Chemical of Interest (COI). This includes plans to mitigate or respond to the consequences of a security incident and to report security incidents internally and externally in a timely manner. An appropriate response should involve not only designated facility emergency response personnel but all facility personnel (including security personnel), as well as local law enforcement and other off-site emergency responders. Response security measures should address the identification of hazards and the proper response plans. Response plans should identify the numbers, capabilities, equipment, and training of the various response personnel. Properly equipped personnel, who understand the potential consequences of a security incident and the need for timely, effective actions, coupled with well-rehearsed response plans reduce the probability of an attack achieving the adversaries' desired goals. Additionally, response personnel practiced in their response plans help ensure that onsite responders and local law enforcement, firefighting, ambulance, mutual aid, and rescue agencies are familiar with the facility and the chemicals stored onsite and that they are not impeded from reaching the location of the security event.

NOTE You may reference Addendum A and the RBPS Guidance Document for more information regarding RBPS requirements and security measures necessary to satisfy the RBPS. The RBPS that satisfy response measures are: RBPS 9, 11, 13, and 14.

Programs and Plans

In this section you are asked to describe the emergency, security, and threat response programs and plans at your facility.

NOTE All facilities should seek to ensure resopnse plans include security elements specific to their security concern and COI(s). If your facility has been tiered for Release COI your facility's crisis management plan should include emergency shutdown plans, evacuation plans, re-entry/recovery plans, and community notification plans, which ensure notification to all community personnel within the impact or affected zone.

Q3.30.010 Emergency/Security Response Organization and Program

Select **Yes** if your facility ***HAS*** an emergency and security response program.

Select **No** if your facility ***DOES NOT HAVE*** an emergency and security response program.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.30.020 Crisis Management Plan

Select **Yes** if your facility maintains a Crisis Management Plan.

Otherwise, select **No.**

*If you select **Yes**, Questions Q3.30.030 and Q3.30.040 will appear. Otherwise, you will skip to Question Q3.30.050.*

Q3.30.030 Crisis Management Plan Details

*If you select **Yes** in Question Q3.30.020, you **MUST** answer this question.*

For each section listed, select **Yes** if it is included in your

facility's Crisis Management Plan. Select **No** if the section is not included.

Select **Yes** for **Other** if your Crisis Management Plan includes sections not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.040 Crisis Management Plan Responsibility

*If you select **Yes** in Question Q3.30.020, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility's Crisis Management Plan covers the responsibility. Select **No** if the responsibility is not covered.

Select **Yes** for **Other** if your facility's Crisis Management Plan covers responsibilities not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.050 Response Drills and Exercises

Select the **frequency** that most accurately describes how often your facility conducts drills and exercises supporting response measures.

Q3.30.060 Other Drills and Exercises

Select the **frequency** that most accurately describes how often your facility conducts other types of drills and exercises.

Q3.30.070 Other Drills and Exercises Description

*If your facility conducts other drills and exercises in Question Q3.30.060, you **MUST** answer this question.*

Enter text up to 4,000 characters to describe the other drills and exercises conducted at your facility.

Q3.30.080 Outreach

For each item listed, select **Yes** if your facility participates in the outreach program. Select **No** if your facility ***DOES NOT*** participate in the outreach program.

Select **Yes** for **Other** if your facility participates in outreach programs that are not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.090 Joint Initiatives

Select **Yes** if your facility participates in joint initiatives.

Otherwise, select **No.**

*If you select **Yes**, Question Q3.30.100 will appear. Otherwise, you will skip to Question Q3.30.110.*

Q3.30.100 Frequency of Joint Exercises

*If you select **Yes** in Question Q3.30.090, you **MUST** answer this question.*

Select the **answer** that most accurately describes your facility's joint exercises.

Q3.30.110 Increased Security Measures during Elevated Threats

Select **Yes** if your facility has a documented process for increasing security measures during periods of elevated threats tied to the National Terrorism Advisory System (NTAS).

Otherwise, select **No.**

NOTE The ability to escalate the level of security measures for periods of elevated threat enables a facility to better protect against known increased threats or generalized increased threats declared by the Federal government. DHS utilizes the NTAS to communicate timely, detailed information about terrorist threats to the public, government agencies, first responders, airports, and other transportation hubs for the private sector. This system alerts at two different levels: elevated and imminent. Facilities are required to increase their security measures when these levels are active as well as when specific threats are identified and reported to them.

Q3.30.120 Elevated Threat Alert

For each item listed, select **Yes** if your facility utilizes the measure when an Elevated Threat Alert is issued. Select **No** if your facility ***DOES NOT*** utilize the measure.

Select **Yes** for **Other** if your facility utilizes measures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.130 Imminent Threat Alert

For each item listed, select **Yes** if your facility utilizes the measure when an Imminent Threat Alert is issued. Select **No** if your facility ***DOES NOT*** utilize the measure.

Select **Yes** for **Other** if your facility utilizes measures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.140 Time Period for Implementing Increased Levels of Security

Select the **time range** which best describes the time in which your facility has the capability to begin implementation of increased levels of security in response to DHS elevating the NTAS threat level and maintain its response measures.

Q3.30.150 Other Elevated Threat Response Elements

Enter text up to 4,000 characters to name and describe other threat response elements at your facility.

Q3.30.160 Facility's Threat Policy

For each item listed, select **Yes** if your facility applies the threat policy. Select **No** if your facility ***DOES NOT*** apply the threat policy.

Select **Yes** for **Other** if your facility applies threat policies not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.170 Training

Select **Yes** if your facility provides threat, vulnerability, or risk training.

Otherwise, select **No.**

Communication

In this section you are asked to describe communication equipment and methods within your facility.

Q3.30.180 Communication Equipment

For each item listed, select **Yes** if your facility utilizes the communication equipment. Select **No** if your facility ***DOES NOT*** utilize the equipment.

Select **Yes** for **Other** if your facility utilizes communication equipment not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.190 Communications

For each item listed, select **Yes** if your facility utilizes the communication system. Select **No** if your facility ***DOES NOT*** utilize the system.

Select **Yes** for **Other** if your facility utilizes communication systems not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.200 Community-Wide Communication

For each item listed, select **Yes** if your facility utilizes the community-wide communication capability. Select **No** if your facility ***DOES NOT*** utilize the capability.

Select **Yes** for **Other** if your facility utilizes community-wide communication capabilities not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

For **Yes** answers you ***MUST*** indicate whether there is a backup power supply for the communication capability.

Q3.30.210 Facility-Wide Communication

For each item listed, select **Yes** if your facility utilizes the facility-wide communication capability. Select **No** if your facility ***DOES NOT*** utilize the capability.

Select **Yes** for **Other** if your facility utilizes facility-wide communication capabilities not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

For **Yes** answers you ***MUST*** indicate if there is a backup power supply for the communication capability.

Onsite Response and Communications

In this section you are asked to describe response and communication capabilities onsite at your facility.

Q3.30.220 Facility Fire Department

Select **Yes** if your facility has an onsite fire department.

Otherwise, select **No.**

If you select **Yes** for this question you ***MUST*** indicate the average number of full time, onsite firefighters. The number must be a positive integer up to 5 digits with no commas or decimals.

Q3.30.230 Facility Ambulance Service Capability

Select **Yes** if your facility has an onsite ambulance service.

Otherwise, select **No.**

If you select **Yes** for this question you ***MUST*** indicate the average number of full time, onsite ambulance service staff.

Q3.30.240 Facility HAZMAT Team

Select **Yes** if your facility has an onsite HAZMAT Team.

Otherwise, select **No.**

Q3.30.250 Shared Emergency Response Capabilities

Select **Yes** if your facility shares emergency response capabilities.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.30.260 will appear. Otherwise, you will skip to Question Q3.30.270.*

Q3.30.260 Response Capability Sharing Entities

*If you select **Yes** in Question Q3.30.250, you **MUST** answer this question.*

In this question you are asked to **Add** information about facilities that share emergency response capabilities.

NOTE *You may reference the CSAT Survey Application User Manual for additional help with adding, editing, or deleting information.*

Other Facility or Entity Name

Enter text up to 200 characters to name the facility that shares emergency response capabilities.

Q3.30.270 Emergency Management Team

Select **Yes** if your facility has an emergency management team.

Otherwise, select **No.**

Q3.30.280 Special Response Capabilities

Select **Yes** if your facility has any special response capabilities such as Bomb Response, CBRNE response, Emergency Medical, Hostage Rescue, Negotiator, Tactical, and/or Toxic Release Response.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.30.290 will appear. Otherwise, you will skip to Question Q3.30.300.*

Q3.30.290 Onsite Special Response Capability

*If you select **Yes** in Question Q3.30.280, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility ***HAS*** the special response capability. Select **No** if your facility ***DOES NOT HAVE*** the capability.

Q3.30.300 Shelter in Place

Select **Yes** if your facility has a safety shelter in place.

Otherwise, select **No.**

Q3.30.310 Facility Emergency Operations Command Center

Select **Yes** if your facility has an Emergency Operations Command Center.

Otherwise, select **No.**

Q3.30.320 Security Command and Control Center

Select **Yes** if your facility has a Security Command and Control Center.

Otherwise, select **No.**

Q3.30.330 Facility Equipment

For each item listed, select **Yes** if your facility utilizes the response equipment. Select **No** if your facility ***DOES NOT*** utilize the response equipment.

Select **Yes** for **Other** if your facility utilizes response equipment not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.340 Process Safeguards

For each item listed, select **Yes** if your facility implements the process safeguards. Select **No** if your facility ***DOES NOT*** implement the safeguard.

Select **Yes** for **Other** if your facility implements process safeguards not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.30.350 Automated Control Systems

Enter a numerical value to describe the percentage of automated control systems capable of rapidly putting COI in a safe and stable condition. The value must be a positive integer with no periods or commas and cannot exceed 100.

Q3.30.360 Emergency Backup Power

Select **Yes** if your facility has backup power for communication capabilities.

Otherwise, select **No.**

Q3.30.370 Emergency Redundant Backup Power

Select **Yes** if your facility has redundant backup power for communication capabilities.

Otherwise, select **No.**

Offsite

In this section you are asked to describe response and communication capabilities of off-site responders to your facility.

Q3.30.380 Local Police Jurisdiction and Capability

This question requires providing multiple data points in various formats in order to complete the answer.

Enter text up to 200 characters to name the local police jurisdiction **AND;**

Enter the local police jurisdiction phone number. The answer must be a 10 digit number with no dashes or periods **AND;**

Enter the average number of full-time police officers in the local jurisdiction. The number must be a positive integer up to 10 digits with no commas or periods.

Q3.30.390 Police Department Drills

Select **Yes** if your local police department ***DOES*** conduct response tests outside of facility drills.

Select **No** if your local police department ***DOES NOT*** conduct response tests outside of facility drills.

Select **Unknown** if you do not know or cannot confirm that your local police department conducts response tests outside of facility drills.

Q3.30.400 Local Fire Jurisdiction and Capability

This question requires providing multiple data points in various formats in order to complete the answer.

Enter text up to 200 characters to name the local fire jurisdiction **AND;**

Enter the local fire jurisdiction phone number**.** The answer must be a 10 digit number with no dashes or periods **AND;**

Enter the average number of full-time firefighters in the local jurisdiction.

Q3.30.410 Local Ambulance Services Jurisdiction and Capability

This question requires providing multiple data points in various formats in order to complete the answer.

Enter text up to 200 characters to name the local ambulance service jurisdiction **AND;**

Enter the local ambulance service jurisdiction phone number **AND;**

Enter the average number of full-time ambulance staff in the local jurisdiction.

Q3.30.420 External Emergency Responder

For each item listed, select **Available Not Dedicated** if your facility has access to a ***SHARED*** responder resource. Select **Available and Dedicated** if your facility has access to a ***DEDICATED*** responder resource. Select **Not Available** if your facility ***DOES NOT HAVE*** access to the responder resource.

Select **Available Not Dedicated** or **Available and Dedicated** for **Other** if your facility has access to any additional shared responder resources not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Not Available** for **Other**.

For **Available Not Dedicated** or **Available and Dedicated** answers, you can use the "Additional Information" text box to provide clarifying details.

If you select **Available Not Dedicated** or **Available and Dedicated** you ***MUST*** indicate the average number of minutes for the responder resource to respond to an incident at the facility. The answer must be a positive integer up to 3 digits with no decimal places or commas.

Response - Planned Measures

In this section, you are asked to describe planned security measures that enhance your facility's response measures.

A planned security measure may be considered by DHS in determining whether an SSP satisfies an applicable RBPS, for example, if the measure:

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

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

Upon submitting your SVA/SSP survey planned measures may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. Of course, if your facility chooses not to provide information about an existing or planned measure that is relevant to the satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Q3.30.430 Planned Measures

Enter up to 4,000 characters in the text box to describe any planned security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS. You ***MUST*** identify the number of months within which your facility intends to implement the planned measure, not to exceed 36 months, after you receive approval of the SSP from DHS. This timeframe should be reasonable and commensurate to the planned action taking place.

Only existing and planned security measures are considered in the formal evaluation of your facility's submitted SSP.

Response - Proposed Measures

In this section, you are asked to describe any proposed security measures that enhance your facility's response measures.

You can provide three types of information for proposed measures:

(1) Proposed Security Measures your facility wants to share with DHS;

(2) Existing Security Measures your facility is proposing to eliminate or remove; and

(3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

You may reference Addendum B for more information for entering proposed security measures.

Q3.30.440 Proposed Measures

Enter up to 4,000 characters in the text box to describe any proposed security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS.

Proposed security measures ***ARE NOT*** considered as part of formal evaluation of your facility's SSP; however, DHS may provide feedback to facilities on the proposed measures listed if they would assist the facility in satisfying a particular RBPS.

Cyber

General Considerations

Facilities must deter cyber sabotage and minimize the consequences of physical events through the protection of cyber systems. This includes preventing unauthorized access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCSs), Industrial Control Systems (ICSs), critical business systems, and other sensitive computerized systems. These cyber systems and the network they operate on are often integrated throughout the operations of chemical facilities. Defending against adverse cyber events is essential to the management of the overall risk for a facility. Comprehensive cybersecurity policies, practices and people are required to handle adverse cyber events and mitigate their effects.

NOTE You may reference RBPS 8 in Addendum A and the RBPS Guidance Document for further information regarding RBPS 8 requirements and security measures necessary to satisfy the RBPS.

Cyber systems that a facility may consider critical for purposes of this RBPS include, but are not limited to, those that monitor and/or control physical processes that contain a COI; are connected to other systems that manage physical processes that contain a COI; or contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a COI. Specific examples of cyber systems that may be considered critical include:

- A control system (including a remotely operated control system) that directly monitors and/or controls manufacturing or other physical processes that contain COI;
- A business system at the headquarters that manages ordering and/or shipping of a COI;
- A business system (at the facility, headquarters, or outsourced) that contains personally identifiable information for those individuals who could be exploited to steal, divert, or sabotage a COI;
- An access control or security monitoring system that is connected to other systems;
- Enterprise resource planning systems that conduct critical functions in support of chemical processes for COI or a COI supply chain activity;
- E-mail and fax systems used to transmit sensitive information related to ordering and/or shipping of a COI;
- A noncritical control system on the same network as a critical control system;
- A sales system that is connected to the data historian for a critical control system;
- A watchdog system (e.g., Safety Instrumented System (SIS)) for a critical control system; and
- A system hosting critical or sensitive information that, if exploited, could result in the theft or diversion of a COI or sabotage its processing (e.g., Web site, intranet).

i Within the security plan, the facility must list all critical cyber assets. The list must include the name of the cyber asset and a brief description, demonstrating how the cyber system may impact the security of the COI. You can modify your facility's critical assets at any time prior to submitting your SVA/SSP survey. You may reference Question Q2.30.010 for defining and editing your facility's critical assets.

Policies and Training

A comprehensive approach to cybersecurity typically will involve policies and procedures that address all cyber systems used by a facility, with certain enhanced security activities directed at critical systems. In this section, you are asked to describe your facility's cyber policies and training procedures.

Q3.40.010 Policies and Training

Select **Yes** if your facility develops and maintains cybersecurity policies and procedures.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.40.020 - Q3.40.050 will appear. Otherwise, you will skip to Question Q3.40.060.*

Q3.40.020 Procedures

*If you select **Yes** in Question Q3.40.010, you **MUST** answer this question.*

Select **the best description** of the facility's approach to ensure the cybersecurity documentation corresponds with the facility's current information technology operating environment.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for your facility's approach to ensure cybersecurity documentation corresponds with its IT operating environment.

Q3.40.030 Security Procedures

*If you select **Yes** in Question Q3.40.010, you **MUST** answer this question.*

Select the **option which best describes** the facility's approach for the cyber change management policy (e.g., new hardware/software, employee access).

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for your facility's cyber change management policy.

Q3.40.040 Audits

*If you select **Yes** in Question Q3.40.010, you **MUST** answer this question.*

Select the **frequency that best describes** when your facility conducts audits that measure compliance with the facility's cybersecurity policies, plans, and procedures and reports the results to senior management.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for your facility's cybersecurity audits procedures.

Q3.40.050 Third Party Cyber Support

*If you select **Yes** in Question Q3.40.010, you **MUST** answer this question.*

Managing relationships with external service providers, business partners, and vendors should be considered so that they do not compromise the security of an organization.

Select **Yes** if your facility ***HAS*** third party support to manage cybersecurity **AND** the facility has procedures or practices in place to ensure these individuals adhere to personnel surety requirements.

Select **No** if your facility ***HAS*** third party support to manage cybersecurity **AND DOES NOT** have procedures or practices in place to ensure these individuals adhere to personnel surety requirements.

Select **Other** if the facility does not have third party support or if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You

can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.060 Employee Training

Select **Yes** if your facility provides cybersecurity training to employees.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.40.070 - Q3.20.100 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.40.070 Training for New Employees

*If you select **Yes** in Question Q3.40.060, you **MUST** answer this question.*

Select the answer that **best describes** the facility's cybersecurity training for new employees.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.080 Cybersecurity Training Process

*If you select **Yes** in Question Q3.40.060, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility conducts the identified cybersecurity training. Select **No** if your facility does not conduct the cybersecurity training.

Select **Yes** for **Other** if your facility has other cybersecurity training not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

*If you select **Yes**, Question Q3.40.090 will appear. Otherwise, you will skip to Question Q3.40.100*

Q3.40.090 Cybersecurity Topics

*If you select **Yes** in Question Q3.40.060, you **MUST** answer this question.*

*If you select **Yes for the listed option "All Employees are trained in general cybersecurity topics"** in Q3.40.080, you **MUST** answer this question.*

For each item listed, select **the frequency** with which your facility provides for the cybersecurity training topic. Select **Other and indicate the frequency** if your facility provides any additional cybersecurity training topics not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Never** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.100 Cyber Training Instructions

Select **Yes** if your facility has a role-based cybersecurity training program for its employees.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.40.110 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.40.110 Cybersecurity Instructional Methods

*If you select **Yes** in Question Q3.40.100, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the cyber training instructional method. Select **No** if your facility does not use the method.

Select **Yes** for **Other** if your facility uses any additional cyber training instructional method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.** You can use the "Additional Information" text box to provide clarifying details for any items listed

IT Personnel

In this section, you are asked to describe your facility's Information Technology (IT) personnel organization.

Q3.40.120 IT Personnel

Select **Yes** if your facility employs an individual(s) responsible for information technology network for the facility.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.40.130 - Q3.40.140 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.40.130 Officials

*If you select **Yes** in Question Q3.40.120, you **MUST** answer this question.*

Select **Yes** if your facility ***HAS*** designated an individual to manage cybersecurity.

Select **No** if your facility ***HAS NOT*** designated an individual to manage cybersecurity.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.140 Separation of Duties

*If you select **Yes** in Question Q3.40.120, you **MUST** answer this question.*

Although people often play multiple roles within an organization, it is generally a good idea to have each individual role and their related security needs defined and separated as much as possible. This distinction allows for natural checks and balances, which is important for preventing human error and internal misuse of systems and information. The goal is to balance security requirements with those of smooth business conduct by implementing an access control scheme that enables both.

Select **Yes** if your facility ***HAS*** different individuals performing systems administration and IT security duties.

Select **No** if your facility ***DOES NOT HAVE*** different individuals performing systems administration and IT security duties.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Network Accounts and Access

In this section, you are asked to describe your facility's IT network accounts and access.

Q3.40.150 Network Accounts and Access

Select **Yes** if your facility maintains accounts and access controls for its IT network.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.40.160 - Q3.40.240 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.40.160 Unique Accounts

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

This question determines whether your facility's system/network users function as a group (e.g., control system operators) and whether user identification and authentication are role based.

Select **Yes** if your facility ***HAS*** implemented compensating security controls (e.g., physical controls).

Select **No** if your facility ***HAS NOT*** implemented compensating security controls (e.g., physical controls).

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.170 Critical Sensitivity Review

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

Select **Yes** if your facility ***DOES*** review and establish security requirements for positions that permit administrative access to systems.

Select **No** if your facility ***DOES NOT*** review and establish security requirements for positions that permit administrative access to systems.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.180 Password Management

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility implements the password management policy or practice. Select **No** if your facility does not implement the policy or practice.

Select **Yes** for **Other** if your facility implements any additional password management policy not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.190 Physical Access to Cyber Systems and Information Storage

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

Select **Yes** if your facility ***HAS*** role-based physical access controls to restrict access to critical cyber assets and media.

Select **No** if your facility ***DOES NOT HAVE*** role-based physical access controls to restrict access to critical cyber assets and media.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.200 Least Privilege

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

Least privilege is the IT security practice where users are only granted access to information, files and/or applications based on their roles and responsibilities within the corporation.

Select **Yes** if your facility ***DOES*** practice the concept of least privilege.

Select **No** if your facility ***DOES NOT*** practice the concept of least privilege.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.210 Access Control Lists

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

To ensure that each employee has the appropriate access to facilities and systems, facilities should actively manage access permissions as employees change roles. For all employees who have departed under adverse circumstances, it is recommended that all access rights (both physical and electronic) be revoked by close of business the same day.

Check **the answers that best describe** how quickly your facility manages its access control lists. You may select more than one answer.

Select **Other** if you have additional access management procedures in place. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.220 External Connections

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

Connectivity is the possibility of transferring data electronically whether through external access, such as the wireless connection, or portable cyber equipment, such as flash drives. Understanding and managing connectivity is typically an essential component of cybersecurity. Because cyber vulnerabilities can be exploited in many ways, connectivity is not as simple as whether or not a wired connection to the Internet is openly in use.

For each item listed, select **Yes** if your facility practices the described external connection requirement. Select **No** if your facility does not use the barrier.

Select **Yes** for **Other** if your facility uses any additional external connection requirement not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.230 System Boundaries

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

System boundaries are any sort of security control designed to limit access to the facility and would include such controls as electronic perimeters.

Select **Yes** if your facility ***DOES*** identify and document system boundaries.

Select **No** if your facilities ***DOES NOT*** identify and document system boundaries.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.240 Access Controls Rules of Behavior

*If you select **Yes** in Question Q3.40.150, you **MUST** answer this question.*

Rules of behavior describe user responsibilities and their expected behavior with regard to information system usage, to include remote access activities (e.g., appropriate Web sites, conduct of personal business).

Select **Yes** if your facility ***DOES*** define the rules of behavior.

Select **No** if your facilities ***DOES NOT*** define the rules of behavior.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Network Operations and System Architecture

In this section, you are asked to describe your facility's network operations and system architecture. A cohesive set of network/system architecture diagrams and documents that describe the nodes, interfaces, and information flows ensures a comprehensive understanding of connectivity, dependency, and security vulnerability based on the system's current operating environment.

Q3.40.260 Network/System Architecture

Select **Yes** if your facility maintains its documented network/system architecture.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.40.27 will appear. Otherwise, you will skip to Question Q3.40.280.*

Q3.40.270 Documented Network/System Architecture

*If you select **Yes** in Question Q3.20.260, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility implements the approach to document network/system architecture. Select **No** if your facility does not use the approach.

Select **Yes** for **Other** if your facility uses any additional network/system architecture documentation approach not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.280 Cyber Asset Identification

Select **Yes** if your facility identifies and evaluates its cyber assets.

Otherwise, select **No**.

NOTE Maintaining a current inventory of hardware (e.g., cyber systems, networks, network devices, media devices), software (e.g., applications), information, and services (e.g., virus checking) on the network has numerous benefits. Network elements can be located, tracked, diagnosed, and maintained with far greater efficiency than if not documented. The vulnerabilities of network elements are identified and evaluated for applicability to the operating environment and then factored into a risk-management decision.

Q3.40.290 System Lifecycle

System lifecycle is the process that describes the design, procurement, installation, operation, and disposal of an information system.

Select **Yes** if your facility incorporates cybersecurity in its system lifecycle.

Otherwise, select **No.**

Q3.40.300 Backup Power for Cyber Systems

Select **Yes** if your facility maintains backup power equipment for the cyber system.

Otherwise, select **No.**

Network Monitoring and Incident Reporting

In this section, you are asked to describe your facility's network monitoring and incident reporting. Network monitoring is critical to identify unauthorized or malicious access, maintain situational awareness, and mitigate risk. An IDS can be used to monitor networks. IDSs are designed to capture network or host traffic, analyze it for known attack patterns, and take specified action when it recognizes an intrusion or attempted intrusion. An IDS can be software or hardware and can be network-based or host-based. Recognizing and logging events and incidents is a critical component of network monitoring.

Q3.40.310 Remote Access to Critical Cyber Assets or Systems

Select **Yes** if your facility has remote access to its critical cyber assets or systems.

Otherwise, select **No.**

Q3.40.320 Protection against Intrusion or Remote Access

Select **Yes** if your facility's system is protected by cybersecurity controls to prevent intrusion or remote access.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.40.330 - Q3.40.360 will appear. Otherwise, you will skip to Question Q.3.40.370.*

Q3.40.330 Network Monitoring

*If you select **Yes** in Question Q3.40.320, you **MUST** answer this question.*

Select **Yes** if your facility ***HAS*** the capability to monitor networks in real-time with immediate alerts.

Select **No** if your facility ***DOES NOT HAVE*** the capability to monitor networks in real-time with immediate alerts.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.340 Network Monitoring Log

*If you select **Yes** in Question Q3.40.320, you **MUST** answer this question.*

Select **the frequency that best describes** your facility's cybersecurity event log review.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **frequency** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.350 Network Monitoring SIS

*If you select **Yes** in Question Q3.40.320, you **MUST** answer this question.*

A Safety Instrumented System (SIS) consists of an engineered set of hardware and software controls which are often used on critical process systems.

For each item listed, select **Yes** if your facility implements an SIS configuration. Select **No** if your facility does not use an SIS configuration.

Select **Yes** for **Other** if your facility uses any additional SIS configuration not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.360 Cybersecurity

*If you select **Yes** in Question Q3.40.320, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility implements the cybersecurity approach. Select **No** if your facility does not implement the approach.

Select **Yes** for **Other** if your facility uses any additional cybersecurity approach not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.40.370 Incident Reporting

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. DHS United States Computer Emergency Readiness Team (US-CERT) is a team within the Department charged with protecting the nation's Internet infrastructure by coordinating defense against and response from cyberattacks.

Select **Yes** if your facility ***HAS*** an incident reporting procedure that ensures significant cyber events are reported to senior management and DHS US-CERT.

Select **No** if your facility ***DOES NOT HAVE*** an incident reporting procedure that ensures significant cyber events are reported to senior management and DHS US-CERT.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.40.380 Post-Incident Measures

Select **Yes** for all of the post-incident measures the facility utilizes.

Select **No** for each measure the facility does not utilize**.**

Q3.40.390 Incident Response

Select **the incident response system** that best describes your facility.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **incident response system** answers, you can use the "Additional Information" text box to provide clarifying details.

Cyber Control and Business Systems

In this section, you are asked to describe your facility's cyber control and business systems and provide additional information related to the integration of those systems with your facility's critical assets. A control system is a term used to describe any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result. The primary purpose of a control system is to measure and control a process. Cyber control systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS). Business systems manage the ordering and/or shipping of potentially dangerous chemicals and may contain personally identifiable information of those individuals who could be exploited to steal or divert potentially dangerous chemicals.

Q3.40.400 Cyber Control Systems

Defining cyber control systems for your facility should be limited to those systems that have the ability to control the process and could result in a release or contamination of COI. Possible examples of these types of systems include SCADA systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS).

Select **Yes** if your facility has a cyber control system related to a critical asset.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.40.410 will appear. Otherwise, you will skip to Question Q3.40.420*

Q3.40.410 Add Control Systems

*If you select **Yes** in Question Q3.40.400, you **MUST** answer this question.*

Click the **Add** button to enter information about each cyber control system within your facility.

NOTE You may reference, the CSAT Survey Application User Manual for additional help with adding, editing or deleting information within a table format question.

Name

Enter text up to 200 characters to name the control system. For example, "Process Control System".

Description

Enter text up to 200 characters to describe the system and its impact on the facility's security posture.

For example, "The control system manages the flow of Chlorine from the railcar to the bleach processing unit. This control system has alarms for leak detection and remotely operated valves that operators can close manually from the control room."

Is the control system offsite?

Select **Yes** if your facility's cyber control system is not stored within your facility's boundaries.

Otherwise, select **No**.

*If you select **Yes** you **MUST** provide the location where the cyber control system is stored.*

Enter the **Physical address**. You may enter an alpha numeric answer up to 200 characters.

AND City; you may enter up to 200 characters

AND State; select the state's name from the dropdown list

AND Zip code; enter a number that is a positive 5 digit integer.

Q3.40.420 Cyber Business System

Cyber business systems include those systems that manage ordering, shipping, receiving, and inventory of chemicals of interest and those systems that are connected to or manage physical security systems, control systems, and other critical systems.

Select **Yes** if your facility has a cyber business system related to a critical asset.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.40.430 will appear. Otherwise, you are finished with this section.*

Q3.40.430 Add Business Systems

*If you select **Yes** in Question Q3.40.420, you **MUST** answer this question.*

Click the **Add** button to enter information about each cyber business system within your facility.

NOTE You may reference, the CSAT Survey Application User Manual for additional help with adding, editing or deleting information within a table format question.

Name

Enter text up to 200 characters to name the business system. For example, “Shipping SAP”

Description

Enter text up to 200 characters to describe the business system and how it impacts the facility’s security posture.

For example, “The SAP system manages the ordering, inventory, and shipping of Hydrogen peroxide.”

Is the control system offsite?

Select **Yes** if your facility’s cybersecurity control system is not stored within your facility’s boundaries (offsite).

Otherwise, select **No**.

If you select **Yes** you ***MUST*** provide the location where the cyber business system is stored.

Enter the **Physical address**. You may enter an alpha numeric answer up to 200 characters.

***AND* City;** you may enter up to 200 characters

***AND* State;** select the state’s name from the dropdown list

***AND* Zip code;** enter a number that is a positive 5 digit integer.

Cybersecurity Other

In this section, you are asked to describe any additional information regarding your facility's cybersecurity management, its processes, process safety, security, product or material stewardship, or business management and control.

Q3.40.440 Cybersecurity Other

Describe other cybersecurity measures that apply to your facility. You can enter up to 4,000 characters.

Cyber - Planned Measures

In this section, you are asked to describe planned security measures that enhance your facility's cybersecurity measures.

A planned security measure may be considered by DHS in determining whether an SSP satisfies an applicable RBPS, for example, if the measure:

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

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

Upon submitting your SVA/SSP survey these planned security measures may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. Of course, if your facility chooses not to provide information about an existing or planned measure that is relevant to the satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Q3.40.450 Planned Measures

Enter up to 4,000 characters in the text box to describe any planned security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS. You ***MUST*** identify the number of months within which your facility intends to implement the planned measure, not to exceed 36 months, after you receive approval of the SSP from DHS. This timeframe should be reasonable and commensurate to the planned action taking place.

Only existing and planned security measures are considered towards the formal evaluation of your facility's submitted SSP.

Cyber - Proposed Measures

In this section, you are asked to describe any proposed security measures that enhance your facility's cybersecurity measures.

You can provide three types of information for proposed measures:

(1) Proposed Security Measures your facility wants to share with DHS;

(2) Existing Security Measures your facility is proposing to eliminate or remove; and

(3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

You may reference Addendum B for more information for entering proposed security measures.

Q3.40.460 Proposed Measures

Enter up to 4,000 characters in the text box to describe any proposed security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS.

Proposed security measures ***ARE NOT*** considered as part of formal evaluation of your facility's SSP; however, DHS may provide feedback to facilities on the proposed measures listed if they would assist the facility in satisfying a particular RBPS.

Security Management

In this SSP subsection, you will describe your facility's security plan for its procedural and management measures.

A facility's security plan cannot be effective without the integration of physical and cyber security measures with procedural security measures. These procedural measures are required to execute all aspects of the security plan. This section covers requirements for maintenance, training, personnel surety, incident reporting and investigation, security organization and officials, and recordkeeping.

NOTE You may reference Addendum A and the RBPS Guidance Document for more information regarding RBPS requirements and security measures necessary to satisfy the RBPS. The RBPS that satisfy detection measures are: RBPS 10, 11, 12, 15, 16, 17 and 18.

System Inspection, Testing, and Monitoring

In this section you are asked to describe the security system management policies and practices at your facility. It is necessary to constantly maintain security systems to ensure their reliability. This includes regularly testing, repairing, and improving the security systems and complying with the manufacturers' instructions and replacement schedules. Performing these activities with diligence increases the likelihood that your security systems will function as expected.

Q3.50.010 Written Procedures

Select **Yes** if your facility has current, written procedures to ensure that all security equipment applicable to the facility (e.g., IDS, CCTV, ACS, lighting, locking mechanisms, process controls/safeguards) is maintained in proper working order.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.50.020 will appear. Otherwise, you will skip to Question Q3.50.030.*

Q3.50.020 Monitoring

*If you select **Yes** in Question Q3.50.010, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility maintains written procedures. Select **No** if your facility ***DOES NOT*** maintain written procedures.

Select **Yes** for **Other** if your facility maintains written procedures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.030 Security Related Equipment Inspection

Select **Yes** if your facility conducts inspections of security equipment.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.50.040 will appear. Otherwise, you will skip to Question Q3.50.050.*

Q3.50.040 Inspection Frequency of Security Related Equipment

*If you select **Yes** in Question Q3.50.030, you **MUST** answer this question.*

For each item listed, select **the frequency** that best describes how often your facility inspects the identified security equipment. Select **Never** if your facility ***DOES NOT*** inspect the security equipment.

Select **the frequency** for **Other** if your facility conducts inspections of security equipment not listed. This may be applicable to facilities who utilize the systems on a daily basis and want to demonstrate daily use as one method of inspection. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Never** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.050 Security System Testing and Maintenance

Select **Yes** if your facility performs testing and maintenance of its security system(s) in accordance to manufacturer's specifications through daily use, inspection, testing and/or a preventative maintenance program.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.50.060 and Q3.50.070 will appear. Otherwise, you will skip to Question Q3.50.080.*

Q3.50.060 Testing Details

*If you select **Yes** in Question Q3.50.050, you **MUST** answer this question.*

For each security system listed, select **Yes** if your facility tests the security system. Select **No** if your facility ***DOES NOT*** test the security system.

Select **Yes** for **Other** if your facility tests security systems not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.070 Maintenance

*If you select **Yes** in Question Q3.50.050, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility conducts the maintenance method. Select **No** if your facility ***DOES NOT*** conduct the maintenance method.

Select **Yes** for **Other** if your facility conducts maintenance methods not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.080 Reporting Non-Routine Incidents

Select **Yes** if your facility ***DOES*** document and promptly report non-routine incidents.

Select **No** if your facility ***DOES NOT*** document or report non-routine incidents.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

For **Yes** or **No** answers, you can use the "Additional Information" text box to provide clarifying details.

Q3.50.090 System Repairs and Compensatory Measures

Select **Yes** if your facility implements compensatory measures in the case of operational deficiency.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.50.100 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.50.100 Temporary/ Compensatory Measures

*If you select **Yes** in Question Q3.50.090, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility implements the temporary/ compensatory measure. Select **No** if your facility ***DOES NOT*** implement the temporary/ compensatory measure.

Select **Yes** for **Other** if your facility implements temporary/ compensatory measures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Training

In this section you are asked to describe security training at your facility. By performing proper security training, exercises, and drills, facility personnel become better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders.

Q3.50.110 Security Awareness and Training Program

Select **Yes** if your facility has implemented a Security Awareness and Training Program (SATP) for facility personnel and/or contractors with security responsibilities.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.50.120 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.50.120 SATP Details

Check **the answers that best describe** the components of your facility SATP. You may select more than one answer.

Select **Other** if you have additional SATP components not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

*If you select **Training**, Questions Q3.50.130 - Q3.50.160 will appear.*

*If you select **Exercises**, Questions Q3.50.170 to Q3.50.200 will appear.*

*If you select **Drills**, Questions Q3.50.210 - Q3.50.230 will appear.*

Otherwise, you are finished with this section.

Q3.50.130 Site Security Officer Training

*If you select **Training** in Question Q3.50.120, you **MUST** answer this question.*

For each item listed, select **the frequency** of your facility Site Security Officer (SSO) training for each topic. Select **Never** if your facility ***DOES NOT*** train its SSO on the topic.

Select **the frequency** for **Other** if your facility conducts SSO training on topics not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Never** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.140 Security Personnel Training

*If you select **Training** in Question Q3.50.120, you **MUST** answer this question.*

For each topic listed, select **the frequency** of your facility's security personnel training for facility personnel and/or contractors. Select **Never** if your facility ***DOES NOT*** train its security personnel on the topic.

Select **the frequency** for **Other** if your facility conducts training on topics not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Never** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.150 All Employees Training

*If you select **Training** in Question Q3.50.120, you **MUST** answer this question.*

For each item listed, select **the frequency** of your facility personnel training for each topic. Select **Never** if your facility ***DOES NOT*** train its personnel on the topic.

Select **the frequency** for **Other** if your facility conducts facility personnel training on topics not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Never** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.160 Training Methods

*If you select **Training** in Question Q3.50.130, you **MUST** answer this question.*

Check **the answers that best describe** the methods implemented for training your facility's SSO. You may select more than one answer.

Select **Other** if you have additional training methods not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.170 Training Exercise Details

*If you select **Exercises** in Question Q3.50.120, you **MUST** answer this question.*

For each exercise description listed, select **Yes** if your facility's security exercises are conducted in the manner described. Select **No** if your facility exercises ***ARE NOT*** conducted as described.

Select **Yes** for **Other** if your facility security exercises contain other elements not described. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.180 Tabletop Exercises Frequency

Tabletop exercises simulate security incidents in an informal, stress-free environment to elicit constructive discussion as participants examine and resolve problems based on existing plans, policies and procedures. There is minimal simulation, no utilization of equipment or deployment of resources, and no time pressures.

Select the **answer** that most accurately describes your facility's tabletop exercises.

Q3.50.190 Frequency of Functional Exercises

Functional exercises fully simulated and interactive exercises. They validate the capability of a group (i.e., protective force) or facility to respond to a simulated event testing one or more procedures and/or function of the facility's security plan. Functional exercises focus on policies, procedures, roles and responsibilities of single or multiple security functions before, during, or after a security related event.

Select the **answer** that most accurately describes your facility.

Q3.50.200 Frequency of Full-Scale Exercises

Full-scale exercises simulate actual emergency conditions and are field exercises designed to evaluate the operational capabilities of the organization's security posture and response capability in a highly stressful environment.

Select the **answer** that most accurately describes your facility's full-scale exercises.

Q3.50.210 Training Drill Details

*If you select **Drills** in Question Q3.50.120, you **MUST** answer this question.*

For each item listed, select **Yes** if your training drills are conducted in the manner described. Select **No** if your facility training drills ***ARE NOT*** conducted as described.

Select **Yes** for **Other** if your facility training drills include other elements not described. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.220 Frequency of Training Drills

*If you select **Drills** in Question Q3.50.120, you **MUST** answer this question.*

Select the **answer** that most accurately describes your facility.

Q3.50.230 Training Drills Topics

*If you select **Drills** in Question Q3.50.120, you **MUST** answer this question.*

Enter text up to 4,000 characters to name and describe any additional drill topics or equipment used at your facility.

Personnel Surety

In this section you are asked to describe RBPS 12 compliance at your facility. This includes background checks to verify identity, criminal history, legal authorization to work, and screening for terrorist ties. A successful background check program can significantly improve a facility's capability to deter, detect, and defend against insider threats or covert attacks. Personnel surety establishes performance standards focused on this critical area and addresses the need for a high-risk chemical facility to ensure that individuals allowed on-site have suitable backgrounds for their level of access.

Affected Individuals

Affected individuals are defined as:

- facility personnel (e.g., employees, contractors[1]) who have or are seeking access, either unescorted or otherwise, to restricted areas or critical assets; and
- unescorted visitors who have or are seeking access to restricted areas or critical assets.

Facilities can define who facility personnel are for their specific situation. Often the facility includes long-term contractors as facility personnel and other contractors such as cleaning or maintenance staff as visitors. At a minimum, facilities must identify all on-site employees as facility personnel.

[1]High-risk facilities may classify particular contractors or categories of contractors either as "facility personnel" or as "visitors."

NOTE Screening for terrorist ties under RBPS 12(iv) has been implemented for Tier 1 and Tier 2 facilities only at this time. Facilities tiered for COI at the Tier 3 and Tier 4 levels will not see questions relating to this part of Personnel Surety until the program has been expanded to include Tier 3 and Tier 4 facilities. For more information on RBPS 12(iv) and the Personnel Surety Program, see 80 FR 79058, Notice of Implementation Chemical Facility Anti-Terrorism Standards Personnel Surety Program published on December 18, 2015 or access the DHS Personnel Surety Program.

Q3.50.240 Personnel Surety Policy

For each item listed, select **Yes** if your facility implements the procedure for Personnel Surety. Select **No** if your facility ***DOES NOT*** implement the procedure.

Select **Yes** for **Other** if your facility implements procedures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.250 Background Check Measure

For each item listed, select **Yes** if your facility implements the background procedure. Select **No** if your facility does not implement the background procedure.

Select **Yes** for **Other** if your facility implements background procedures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.260 Background Investigations

Select **Yes** if your facility has identified grounds for denying access or employment. This may include specific disqualifying criteria or a policy/procedure for reviewing background checks and making hiring or access decisions.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.270 Background Investigation Recurrence

Select **Yes** if your facility conducts background investigations periodically on existing personnel.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.50.280 will appear. Otherwise, you will skip to Question Q3.50.290.*

Q3.50.280 Background Investigation Frequency

*If you select **Yes** in Question Q3.50.270, you **MUST** answer this question.*

Select the **interval frequency that best describes** your facility's repeated background investigations.

Select **Other** if your facility repeats background investigations at a frequency not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.290 Access Control

For each item listed, select **Yes** if your facility implements the access control measure. Select **No** if your facility ***DOES NOT*** implement measure.

Select **Yes** for **Other** if your facility implements access control measures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.300 Background Check Program Audit

Select **Yes** if your facility conducts audits of the background check program.

Otherwise, select **No.**

*If you select **Yes,** Question Q3.50.310 will appear. Otherwise, you will skip to Question Q3.50.320.*

Q3.50.310 Background Check Program Audit Percentage

*If you select **Yes** in Question Q3.50.300, you **MUST** answer this question.*

Select the percentage range that best describes your facility's background check audit.

Q3.50.320 Types of Affected Individuals

Check **the answers that best describe** the types of affected individuals at your facility. You may select more than one answer.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.330 Personnel Surety Options

*If your facility is a Tier 1 or 2 facility, you will see this question and all follow-on questions related to screening for terrorist ties and **MUST** answer this question. If your facility is a Tier 3 or 4 facility, you will not see these questions until the Personnel Surety Program is deployed to Tier 3 and Tier 4 facilities.*

Check **the answers that best describe** the options currently used or planned to be used to screen affected individuals for terrorist ties. You may select more than one answer.

For **each item** selected, you ***MUST*** identify which affected individuals are screened under the selected option. This should be a clear description of the affected individual population, but should not be a list of individual names. For example, a facility may select Option 1 for "all facility personnel working within the chemical warehouse" and Option 2 for "all drivers and contractors". You can enter up to 4,000 characters.

*If you select **Option 1**, Questions Q3.50.340 - Q3.50.360 will appear.*

*If you select **Option 2**, Questions Q3.50.340 and Q3.50.370 - Q3.50.400 will appear.*

*If you select **Option 3**, Questions Q3.50.340 and Q3.50.410 - Q3.50.470 will appear.*

*If you select **Option 4**, Questions Q3.50.340 and Q3.50.480 - Q3.50.540 will appear.*

*If you select **Other**, you must answer Question Q3.50.340 will appear.*

NOTE For more details describing the personnel surety options to comply with RBPS 12(iv), see the Personnel Surety Program Notice of Implementation.

Q3.50.340 Personnel Surety Assertions

For each item listed, select **Yes** if your facility acknowledges the RBPS 12(iv) item. Select **No** if your facility ***DOES NOT*** acknowledge the RBPS 12(iv) item.

Q3.50.350 Option 1 Affirmation

*If you select **Option 1** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility affirms affected individuals submitted under Option 1 are provided appropriate notices.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details.

Q3.50.360 Option 1 - Notification to DHS

*If you select **Option 1** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility plans to notify DHS via CSAT when affected individuals no longer have access to restricted areas and/or critical assets.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.370 Option 2 Affirmation

*If you select **Option 2** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility affirms affected individuals submitted under Option 2 are provided appropriate notices.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.380 Option 2 - Vetting Programs

*If you select **Option 2** in Question Q3.50.330, you **MUST** answer this question.*

In this question you are asked to **Add** information about vetting programs. You may choose to add vetting programs which are allowable under Option 2 to include TWIC, HME, and Trusted Traveler Programs.

NOTE You may reference, the CSAT Survey Application User Manual for additional help with adding, editing, or deleting information.

Program

Enter text up to 200 characters to name the program.

For example, "TWIC."

Types of facility personnel or unescorted visitors utilizing the program

Enter text up to 200 characters to name and describe the personnel and visitors who will utilize this program.

For example, "Delivery Personnel".

Q3.50.390 Option 2 - Verification of Individual

*If you select **Option 2** in Question Q3.50.330, you **MUST** answer this question.*

Enter text up to 4,000 characters to describe procedures for individuals whose enrollment cannot be verified in another Department Terrorist Screening Database vetting program.

Q3.50.400 Option 2 - Timeframe for Follow-On Action

*If you select **Option 2** in Question Q3.50.330, you **MUST** answer this question.*

Select the **timespan that best describes** your facility's follow-on action if DHS is unable to verify an affected individual is enrolled in other vetting programs.

Select **Other** if your facility timeframe for follow-on action is not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

NOTE The Personnel Surety Program Application allows facilities to automatically revert Option 2 affected individuals to Option 1 if DHS is unable to verify an affected individual's enrollment in the designated program. This would allow for an immediate action to address this question.

Q3.50.410 Option 3 - Notice to Affected Individuals

If you select Option 3 in Question Q3.50.330, you MUST answer this question.

Select **Yes** if your facility provides notice to affected individuals submitted under Option 3.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details.

Q3.50.420 Option 3 - Trained Individual(s) for TWICs Verification

If you select Option 3 in Question Q3.50.330, you MUST answer this question.

Select **Yes** if your facility has trained individual(s) in the Transportation Worker Identification Credentials (TWIC) verification processes.

Otherwise, select **No.**

Q3.50.430 Option 3 - TWIC Revalidation Frequency

If you select Option 3 in Question Q3.50.330, you MUST answer this question.

Select the **answer** that most accurately describes your facility.

Select **Other** if your TWIC revalidation timeframe is not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.440 Option 3 - Modes for Verifying TWIC

If you select Option 3 in Question Q3.50.330, you MUST answer this question.

Select **Yes** if your facility has procedures to describe TWIC Reader settings utilized in the validation of TWIC credentials.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.450 Option 3 - Visual Verification of TWIC

*If you select **Option 3** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility conducts visual validation along with electronic validation of TWIC credentials.

Otherwise, select **No.**

If you select **Yes** for this question you ***MUST*** indicate which methods are used for visual validation. Select all options that apply.

Q3.50.460 Option 3 - TWIC Reader Malfunction

If you select Option 3 in Question Q3.50.330, you MUST answer this question.

Enter text up to 4,000 characters to describe procedures for affected individuals whose TWIC cannot be verified at your facility.

Q3.50.470 Option 3 - Timeframe for Follow-On Action

If you select Option 3 in Question Q3.50.330, you MUST answer this question.

Select the **timespan that best describes** your facility's follow-on action if your facility is unable to verify an affected individual's credentials.

Select **Other** if your facility timeframe for follow-on action is not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

Q3.50.480 Option 4 - Notice to Affected Individuals

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility provides notice to affected individuals submitted under Option 4.

Otherwise, select **No.**

You can use the "Additional Information" text box to provide clarifying details.

Q3.50.490 Option 4 - Individual to Verify Credentials

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility has designated and trained individuals to verify documents and credentials.

Otherwise, select **No.**

Q3.50.500 Option 4 - Policy for Visual Verification

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

Select **Yes** if your facility maintains a policy of which documents and credentials are acceptable for visual verification.

Otherwise, select **No.**

Q3.50.510 Option 4 - Types of Credentials Accepted by Facility

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

In this question you are asked to **Add** information about credential types accepted by the facility.

Credential or document

Enter text up to 200 characters to name the credential or document.

For example, "TWIC."

Types of facility personnel or unescorted visitors utilizing the program

Enter text up to 200 characters to name the type of personnel that utilize the credential.

For example, "Delivery Personnel".

NOTE You may reference, the CSAT Survey Application User Manual for additional help with adding, editing or deleting information.

Q3.50.520 Option 4 - Types of Credentials Not Accepted by Facility

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

In this question you are asked to **Add** information about credential types ***NOT*** accepted by the facility.

Credential or document

Enter text up to 200 characters to name the credential or document.

For example, "HME".

NOTE You may reference, the CSAT Survey Application User Manual for additional help with adding, editing or deleting information.

Q3.50.530 Option 4 - Visual Verification of Credentials

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

Check **the answers that best describe** your facility methods for visual verification. You may select more than one answer.

You can use the "Describe" text box to provide clarifying details for any items listed.

Q3.50.540 Option 4 - Procedures if Unable to Visually Verify Credentials

*If you select **Option 4** in Question Q3.50.330, you **MUST** answer this question.*

Enter text up to 4,000 characters to describe procedures for TWIC credentials that cannot be visually verified.

Q3.50.550 Other Methods

*If you select **Other** in Question Q3.50.330, you **MUST** answer this question.*

Enter text up to 4,000 characters to describe other procedures for satisfying RBPS 12(iv).

Reporting Significant Security Incidents

In this section, you are asked to describe the security incident reporting and training programs at your facility. Facilities should develop and maintain an incident reporting and investigation program in order to promptly and adequately report all significant security incidents to the appropriate facility personnel, local law enforcement entities, and DHS.

The following security incidents should be considered as reportable to facility security personnel, local law enforcement, and DHS (via the National Infrastructure Coordinating Center (NICC) at nicc@dhs.gov or at 202 282 9201):

- unauthorized, successful or unsuccessful breaches of the perimeter;
- unauthorized, successful or unsuccessful breaches of the critical asset(s);
- COI inventory control issues;
- suspected theft of COI;
- unauthorized release of COI;
- sabotage or contamination of COI;
- suspicious orders for COI; and
- any act of tampering with malicious intent to critical physical or cyber asset(s).

If a significant security incident is detected while in progress, the first call should be to local law enforcement and emergency responders via 911. If the incident has concluded but an immediate emergency response is necessary, it is recommended that a facility report the incident immediately to local first responders via 911. Once the incident has concluded and any subsequent emergencies have been mitigated, a facility should use a nonemergency number to inform local first responders and DHS if they have not already been contacted. Within DHS, incidents should be reported to the NICC. Additionally, control systems community submissions of cyber incidents and vulnerabilities to Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is essential to its ability to provide national level situational awareness for the nation's critical control systems cyber security status. ICS-CERT coordinates with US-CERT and other partners to develop Joint Security Awareness Reports (JSARs) to provide situational awareness for the public on cybersecurity issues. Submissions can be made through the ICS-CERT Web site Home page. Another contact resource your facility may wish to communicate with is its local FBI Field Office, whose phone number can be found online at www.fbi.gov/contact/fo/focities.htm.

Q3.50.560 Procedures for Security Incidents

For each item listed, select **Yes** if your facility implements the procedure for security incidents. Select **No** if your facility ***DOES NOT*** implement the procedure.

Select **Yes** for **Other** if your facility maintains security incident procedures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

NOTE Facilities should have written procedures which define incident reporting and investigation protocols, include the types of incidents to report, identify to whom to report incidents, and list the responsibilities of all individuals with reporting and investigation roles.

Q3.50.570 Reporting Procedures

Select **Yes** if your facility has documented procedures for reporting suspicious activities to its security personnel and, if appropriate, local law enforcement or DHS.

Otherwise, select **No.**

Q3.50.580 Significant Security Incidents

For each item listed, select **Yes** if your facility defines the incident as significant. Select **No** if your facility ***DOES NOT*** define the incident as significant.

Select **Yes** for **Other** if your facility defines incidents not listed as significant. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select

No for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.590 Training Frequency

For each topic listed, select **the frequency that best describes how often** your facility conducts training. Select **Never** if your facility ***DOES NOT*** conduct training for the topic.

Select **the frequency** for **Other** if your facility conducts training for topics not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **Never** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.600 Near Miss Security Incidents

For each item listed, select **Yes** if your facility utilizes the procedure for near miss security incidents. Select **No** if your facility ***DOES NOT*** utilize the procedure.

Select **Yes** for **Other** if your facility utilizes near miss security incident procedures not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Investigating Significant Security Incidents

Facilities should have a security incident investigation program to thoroughly investigate all significant security incidents. The personnel who conduct such investigations, whether internal or third party personnel, must be properly trained and qualified. In this section, you are asked to describe your facility's investigation program.

Q3.50.610 Investigation of Significant Security Incidents

For each item listed, select **Yes** if your facility utilizes the investigation method for security incidents. Select **No** if your facility ***DOES NOT*** utilize the investigation method for security incidents.

Select **Yes** for **Other** if your facility utilizes investigation methods not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.620 Data Collected

Enter text up to 4,000 characters to describe data collected during the security incident investigation process.

NOTE Suggested data/facts to collect during the investigation process include: Date/time incident occurred, was reported and the investigation occurred; Facility specific investigation/indexing case number; Location; Investigator information; Type of Incident, Narrative Description of Incident; Responding agency; Persons/Vehicles of interest involved in incident; Formal internal investigation date completed; and Action items from investigation.

Q3.50.630 Investigations

For each qualification listed, select **Yes** if the type of investigations is utilized at your facility for security incidents. Select **No** if your facility ***DOES NOT*** utilize the type of investigation.

Select **Yes** for **Other** if your facility utilizes investigation types not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.640 Investigation Lessons Learned

Select **Yes** if your facility manages and maintains lessons learned from security incident investigations.

Otherwise, select **No.**

Q3.50.650 Dissemination of Investigation Lessons Learned

Select **Yes** if your facility ***DOES*** disseminate security incident investigation lessons learned to employees.

Select **No** if your facility ***DOES NOT*** disseminate security incident investigation lessons learned to employees.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Officials and Organizations

Facilities should identify the office and officials within the company responsible for security and CFATS compliance. The manner in which a facility structures its security organization to meet this specific requirement will likely depend on its complexity and its ownership structure. A larger, more complex facility is likely to have a more complex organization responsible for compliance than a smaller facility and also is more likely to employ an individual whose principal job responsibility is facility security.

Facilities should designate a Site Security Officer (SSO), Alternate SSO, Cyber Security Officer, and where applicable, a Corporate Security Officer. Those designated should be given clear responsibilities and the qualifications and training to perform them. Individuals may serve in more than one role; however, the SSO and Alternate SSO should be different people where possible. Qualifications for being an SSO (or equivalent) should include:

- Understanding the security organization of the facility;
- Understanding the requirement to comply with the CFATS RBPSs;
- Experience in emergency preparedness, response, and planning for disasters;
- Familiarity with responsibilities and functions of local, state, and federal law enforcement agencies; and
- Ability to recognize characteristics and behavioral patterns of persons who are likely to threaten security.

In this section, you are asked to describe your facility's security organization structure and policy.

Q3.50.660 Security Organization Policy

For each item listed, select **Yes** if your facility employs a security policy or element. Select **No** if your facility ***DOES NOT*** employ the security policy or element.

Select **Yes** for **Other** if your facility employs security policies not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.670 SSO Responsibilities

For each item listed, select **Yes** if your facility Site Security Officer (SSO) has this responsibility. Select **No** if your facility SSO ***DOES NOT*** have this responsibility.

Select **Yes** for **Other** if your facility SSO has security responsibilities not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.680 SSO Qualifications

For each item listed, select **Yes** if your facility Site Security Officer (SSO) satisfies this qualification. Select **No** if your facility SSO ***DOES NOT*** satisfy this qualification.

Select **Yes** for **Other** if your facility SSO satisfies qualifications not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.690 Security Organization

Select **Yes** if your facility has established a security organization.

Otherwise, select **No.**

*If you select **Yes,** Questions Q3.50.700 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.50.700 Security Organization

*If you select **Yes** in Q3.50.690, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility security organization has these characteristics. Select **No** if your facility SSO ***DOES NOT*** have these characteristics.

Records

Pursuant to 6 CFR Part 27.255, recordkeeping requirements, covered facilities must create, maintain, protect, store, and make available for inspection by DHS records related to its security program. This includes, but is not limited to, specific recordkeeping requirements to include:

(1) *Training*. For training, the date and location of each session, time of day and duration of session, a description of the training, the name and qualifications of the instructor, a clear, legible list of attendees to include the attendee signature, at least one other unique identifier of each attendee receiving the training, and the results of any evaluation or testing.

(2) *Drills and exercises*. For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, a list of equipment (other than personal equipment) tested or employed in the exercise, the name(s) and qualifications of the exercise director, and any best practices or lessons learned which may improve the Site Security Plan;

(3) *Incidents and breaches of security*. Date and time of occurrence, location within the facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response;

(4) *Maintenance, calibration, and testing of security equipment*. The date and time, name and qualifications of the technician(s) doing the work, and the specific security equipment involved for each occurrence of maintenance, calibration, and testing;

(5) *Security threats*. Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(6) *Audits*. For each audit of a covered facility's Site Security Plan (including each audit required under § 27.225(e) or Security Vulnerability Assessment, a record of the audit, including the date of the audit, results of the audit, name(s) of the person(s) who conducted the audit, and a letter certified by the covered facility stating the date the audit was conducted.

(7) *Letters of Authorization and Approval*. All Letters of Authorization and Approval from the Department, and documentation identifying the results of audits and inspections conducted pursuant to § 27.250.

In this section you are asked to describe records management and administration at your facility.

Q3.50.710 Affirmation

Check the **affirmation statement** if your facility manages and maintains records in compliance with the CFATS Rule.

If you **do not check** the affirmation statement you **MUST** describe how your facility satisfies recordkeeping requirements in the text box. You can enter up to 4,000 characters.

Q3.50.720 Records Creation

Select **Yes** if your facility ***DOES*** create written records.

Select **No** if your facility ***DOES NOT*** create written records.

Select **Other** if the choices available do not fit or do not fully describe your facility. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

*If you select **Yes,** Questions Q3.50.730 - Q3.50.750 will appear. Otherwise, you are finished with this subsection of the SVA/SSP survey.*

Q3.50.730 Records Content

*If you select **Yes** in Q3.50.720, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility prepares the record. Select **No** if your facility ***DOES NOT*** prepare the record.

Q3.50.740 Records Disposal

*If you select **Yes** in Q3.50.720, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility uses the method to dispose of its records. Select **No** if your facility ***DOES NOT*** use the method.

Select **Yes** for **Other** if your facility utilizes a record disposal method not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text

box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Q3.50.750 Availability of Records

*If you select **Yes** in Q3.50.720, you **MUST** answer this question.*

For each item listed, select **Yes** if your facility can produce the records in the described scenario. Select **No** if your facility ***CANNOT*** produce the record in the scenario listed.

Select **Yes** for **Other** if your facility produces its records in other manners/scenarios not listed. If you select this option, you ***MUST*** provide an explanation in the "Additional Information" text box. You can enter up to 4,000 characters. Otherwise, select **No** for **Other**.

You can use the "Additional Information" text box to provide clarifying details for any items listed.

Security Management- Planned Measures

In this section, you are asked to describe planned security measures that enhance your facility's security management measures.

A planned security measure may be considered by DHS in determining whether an SSP satisfies an applicable RBPS, for example, if the measure:

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

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

Upon submitting your SVA/SSP survey these may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. Of course, if your facility chooses not to provide information about an existing or planned measure that is relevant to the satisfaction of one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

Q3.30.760 Planned Measures

Enter up to 4,000 characters in the text box to describe any planned security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS. You ***MUST*** identify the number of months, not to exceed 36 months, within which your facility intends to implement the planned measure after you receive approval of the SSP from DHS. This timeframe should be reasonable and commensurate to the planned action taking place.

Only existing and planned security measures are considered in the formal evaluation of your facility's submitted SSP.

Security Management- Proposed Measures

In this section, you are asked to describe any proposed security measures that enhance your facility's security management measures.

You can provide three types of information for proposed measures:

(1) Proposed Security Measures your facility wants to share with DHS;

(2) Existing Security Measures your facility is proposing to eliminate or remove; and

(3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

You may reference Addendum B for more information for entering proposed security measures.

Q3.50.770 Proposed Measures

Enter up to 4,000 characters in the text box to describe any proposed security measures that your facility wants DHS to consider in determining the satisfaction of the RBPS.

Proposed security measures ***ARE NOT*** considered as part of formal evaluation of your facility's SSP; however, DHS may provide feedback to facilities on the proposed measures listed if they would assist the facility in satisfying a particular RBPS.

Optional Supporting Documentation

You have the option to provide DHS with supporting documentation for your SSP. To upload additional supporting documentation, select the "Browse / Choose File" button to locate the file(s) on your computer or your facility's network. Once you have browsed for all of your files, select the "Upload" button to upload all the files identified.

Do not upload password protected files.

NOTE See the CSAT Survey Application User Manual for instructions in using the Upload files function.

Addendum A – General Concepts

RBPS

Facilities must identify measures to satisfy each requirement within their SSP/ASP/EAP in order to satisfy the entirety of the RBPS (See 6 CFR § 27.230). You may reference the RBPS Guidance Document for term definitions and more details in implementing each RBPS. For reference, the RBPS are included below.

RBPS 1: Restrict Area Perimeter. Secure and monitor the perimeter of the facility.

RBPS 2: Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility.

RBPS 3: Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including:

(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and

(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourage abuse through established disciplinary measures.

RBPS 4: Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(ii) Deter attacks through visible, professional, well-maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced-value targets;

(iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and

(iv) Delay an attack for a sufficient period of time to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.

RBPS 5: Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.

RBPS 6: Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals.

RBPS 7: Sabotage. Deter insider sabotage.

RBPS 8: Cyber. Deter cyber sabotage, including by preventing unauthorized on-site or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs); critical business systems; and other sensitive computerized systems.

RBPS 9: Response. Develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders.

RBPS 10: Monitoring. Maintain effective monitoring, communications, and warning systems, including:

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions.

RBPS 11: Training. Ensure proper security training, exercises, and drills of facility personnel.

RBPS 12: Personnel Surety. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including:

(i) Measures designed to verify and validate identity;

(ii) Measures designed to check criminal history;

(iii) Measures designed to verify and validate legal authorization to work; and

(iv) Measures designed to identify people with terrorist ties.[1]

RBPS 13: Elevated Threats. Escalate the level of protective measures for periods of elevated threat.

RBPS 14: Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities, or risks identified by the Assistant Secretary for the particular facility at issue.

RBPS 15: Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials.

RBPS 16: Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site.

RBPS 17: Officials and Organization. Establish official(s) and an organization responsible for security and for compliance with these standards.

RBPS 18: Records. Maintain appropriate records.

[1] All facilities, in all tiers, must comply with subparts (i), (ii), and (iii) of RBPS 12 (See 6 CFR §27.230(a)(12)) as part of their SSPs. Facilities will only be required to comply with RBPS 12(iv) after certain other events have occurred, however. Compliance with RBPS 12(iv) will be required for Tiers 1 and 2 upon approval of an Information Collection Request under the Paperwork Reduction Act, and upon notification to facilities by DHS that the CFATS Personnel Surety Program (i.e., the program enabling compliance with RBPS 12(iv)) has been implemented. DHS will seek to implement RBPS 12(iv) for Tiers 3 and 4 after the CFATS Personnel Surety Program has been implemented for Tiers 1 and 2, and will update its Information Collection Request and publish new Paperwork Reduction Act materials prior to implementation for Tiers 3 and 4.

Addendum B – Proposed Security Measures

You can provide three types of information for proposed measures:

(1) Proposed Security Measures your facility wants to share with DHS;

(2) Existing Security Measures your facility is proposing to eliminate or remove; and

(3) Existing or Planned Security Measures the facility does not want DHS to consider during the evaluation of the facility's SSP.

Entering Proposed Security Measures

If your facility chooses to share its proposed security measures with DHS, then you should enter a description of the proposed security measure. Label each proposed security measure using "Proposed Security Measure X" where the X would be a number for the Proposed Security Measure.

A sample entry for a Proposed Security Measures could be: "Proposed Security Measure 1 – Install new 8 feet high chain link fence with one (1) foot high barbed wire topping; Proposed Security Measure 2 – Install 2 CCTV cameras at the facility's main gate." The facility can provide as much detail as necessary to convey each Proposed Security Measure to DHS.

Entering Proposals to Eliminate Security Measures

Existing security measures which each covered facility describes or lists in its CSAT SSP submission may become enforceable components of that facility's final SSP upon approval of the SSP by DHS. However, this section provides the opportunity to disclose that certain existing security measures are proposed to be removed or eliminated in the future. Of course, if a facility chooses to eliminate an existing security measure that is relevant to one or more CFATS RBPS, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

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

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

Existing and planned security measures described or listed in the SVA/SSP submission may become enforceable components upon approval of the SSP by DHS. However, this section of the CSAT SSP tool will provide facilities the opportunity to propose that certain existing and/or planned security measures identified in this tool not be considered by DHS in evaluating its SSP for approval. Of course, if a facility chooses not to include an existing or planned measure that is relevant to satisfaction of one or more CFATS RBPS in its SSP, it is possible that the facility's SSP, as submitted, may not satisfy the applicable RBPS.

If your facility would like to identify existing or planned security measures in the CSAT SSP tool for a specific RBPS, but does not want DHS to consider those measures during its evaluation of the facility's SSP, you facility should make a note of the question numbers that correspond to those particular security measures.

Use the proposed text box to enter a description of the security measures the facility does not want DHS to consider. Label each security measure not to be included by using "Security Measure Not to be Included in question [Q3.##.###]". A sample entry could be, "Security Measure Not to be Included in [Q3.20.070] Facility does not want its perimeter fence considered by DHS during evaluation of its SSP; Security Measure Not to be Included in [Q3.20.060] Facility does not want its clear zone considered by DHS during evaluation of its SSP.

Acronym List

ACS	Access Control System
ASP	Alternative Security Program
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
DCS	Distributed Control Systems
DHS	U.S. Department of Homeland Security
EAP	Expedited Approval Program
HME	Hazardous Materials Endorsement
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection System
IFR	Interim Final Rule
N/A	Not Applicable
NICC	National Infrastructure Coordinating Center
PDF	Portable Document Format
RBPS	Risk-Based Performance Standards
SCADA	Supervisory Control and Data Acquisition
SSO	Site Security Officer
SSP	Site Security Plan
STQ	Screening Threshold Quantity
SVA	Security Vulnerability Assessment
TS	Top-Screen
TWIC	Transportation Worker Identification Credential
US-CERT	United States Computer Emergency Response Team