Guidance Document

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

Document Summary: The following document contains specific steps facilities that choose to take part in the Expedited Approval Program (EAP) should take if they wish to take advantage of the benefits of that program.

Document Title: DHS Guidance for the Expedited Approval Program

Issued by: Infrastructure Security Compliance Division, Cybersecurity and Infrastructure Security Agency

Date of Issuance/Revision: May 6, 2015

Affected parties: Owners and operators of facilities subject to CFATS requirements assigned a final Tier 3 or 4.

Statutory or regulatory provisions interpreted: 6 U.S.C. 622(c)(4)

Document Identification Number: CISA-CFATS-003

Link: www.cisa.gov/publication/cfats-expedited-approval-program

DHS Guidance for the Expedited Approval Program

Table of Contents

Overview

The Department of Homeland Security (DHS or the Department) regulates high-risk chemical facilities under the Chemical Facility Anti-Terrorism Standards Program (CFATS), 6 C.F.R. Part 27. CFATS was created pursuant to Section 550 of the Homeland Security Appropriations Act of 2007, P.L 109-295, which gave DHS regulatory authority over security at high-risk chemical facilities. Under CFATS, facilities that have been finally determined by DHS to be high-risk are required to develop and implement security plans that meet applicable Risk-Based Performance Standards (RBPS).

Congress re-authorized CFATS in 2014 through the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (the Act), P.L. 113-254 (6 U.S.C. § 621, et seq.). While the Act preserves most of the existing CFATS regulations, some aspects of the program are changing as a result of the new law.

One new creation of the Act is a process for high-risk chemical facilities assigned a final Tier 3 or 4 to receive expedited approval of their Site Security Plans (SSP). The Act directs DHS to issue prescriptive guidance for facilities that choose to submit SSPs as part of the Expedited Approval Program that "identifies specific security measures that are sufficient to meet the risk-based performance standards." See 6 U.S.C § 622(c)(4)(B)(i). This document provides the statutorily required guidance to facilities choosing to file under the Expedited Approval Program, which includes specific security measures that are sufficient to meet the RBPS the facilities must satisfy under 6 CFR § 27.230.

How to Use this Guidance Document

This guidance document was specifically developed to meet the requirements of 6 U.S.C. 622(c)(4)(B) and must be used by each chemical facility that submits an Expedited Approval Program SSP. Although this guidance discusses security measures specific to the Expedited Approval Program, Tier 3 and 4 chemical facilities can use this document to help gain a better understanding of security measures which could be used to meet the RBPS and to help identify and select processes, measures, and activities that they may choose to implement to secure and monitor their facility.

Timelines

In general, facilities assigned a final Tier 3 or 4 may elect to submit a security plan pursuant to the Expedited Approval Program using this guidance document. See 6 U.S.C. § 622(c)(4)(A). Facilities assigned a final Tier 3 or 4 prior to December 18, 2014 (the date of enactment of the Act) that choose to submit a SSP and certification under the Expedited Approval Program must submit the security plan not later than November 13, 2015. Facilities that are assigned final Tier 3 or 4 after December 18, 2014 have until November 13, 2015, or 120 days after their assignment to Tier 3 or 4, whichever date is later. See 6 U.S.C. § 622(c)(4)(D).

Further, any facility that elects to submit under the new Expedited Approval Program must notify DHS of its intention to do so at least 30 days prior to submitting the security plan and certification. See 6 U.S.C. § 622(c)(4)(D)(iii). This notification can be made via the Department's Chemical Security Assessment Tool (CSAT) system or letter sent to:

Director, Infrastructure Security Compliance Division
Office of Infrastructure Protection
Department of Homeland Security
Mail Stop 0610
245 Murray Lane
Washington, D.C. 20528

Risk-Based Performance Standards (RBPS)

Facilities must identify measures to satisfy each requirement within this guidance document in order to satisfy the entirety of the RBPS (See 6 CFR § 27.230). 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.

[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.

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.

Many RBPS have overlapping requirements and are grouped to most efficiently describe the requirements of the CFATS program. This document is organized into overarching security objectives, which collectively account for all of the requirements of the RBPS as described in the below table:

		Overarching Security Objectives				
		Detection	**Delay**	**Response**	**Cyber Security**	**Security Management**
Risk-Based Performance Standards	**Restrict Area Perimeter**	**X**	**X**			
	Secure Site Assets	**X**	**X**			
	Screen and Control Access	**X**	**X**			
	Deter, Detect, and Delay	**X**	**X**			
	Shipping, Receipt and Storage	**X**	**X**			
	Theft and Diversion	**X**	**X**			
	Sabotage	**X**	**X**			**X**
	Cyber				**X**	
	Response			**X**		
	Monitoring					**X**

	Training			**X**		**X**
	Personnel Surety					**X**
	Elevated Threats			**X**		
	Specific Threats			**X**		
	Reporting of Significant Security Incidents					**X**
	Significant Security Incidents and Suspicious Activities					**X**
	Officials and Organization					**X**
	Records					**X**

Facilities choosing to submit an SSP as part of the Expedited Approval Program must include security measures which cover all RBPS and must review all security objectives to ensure that their plan meets the requirements of all RBPS.

The programs and processes a facility ultimately chooses to implement to meet the RBPS under the Expedited Approval Program must be described within the SSP developed by the facility pursuant to the Act. Facilities utilizing this program must develop their SSP utilizing the guidance herein.[2]

Material Deviations

A security plan submitted through the Expedited Approval Program must comply with the guidance set forth in this document. If a facility chooses a security measure that materially deviates from a measure specified in the guidance, then the facility's SSP must identify the deviation for the specific security measure and explain how the new measure meets the relevant RBPS. See 6 U.S.C. 622(c)(4)(B)(ii).

[2] The Act also permits DHS to develop a template, which a facility could adopt to participate in the EAP by utilizing a template developed by DHS (see 6 U.S.C. §§ 622(c)(4)(A)(ii) & (H)); however, at this time, DHS has not completed the development of any such templates for use as part of this program. Therefore, at this time, a facility choosing to participate in the EAP must use this guidance document.

Material deviations are set forth for each specific required security measure throughout this guidance. Specific examples of material deviations are also provided. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), a facility must explain how a materially deviating measure accomplishes the security outcome(s) required by the relevant RBPS. In light of the overlap of the RBPS as explained in the above chart, DHS has identified the relevant portions of the applicable RBPS for each measure. For each material deviating measure, a facility must explain how the measure meets each of these elements of the RBPS. See Attachment 2 for an example of how to correctly identify a material deviation.

The guidance document also provides examples of deviations that would not be considered material. These are provided in the form of options and in the form of broader language to permit non-material deviations within the required measures. The security measures herein are prescriptive, in that a facility must either choose a measure listed or choose to materially deviate; however, DHS believes that there is considerable latitude for non-material deviations within the required measures. For instance, when a facility chooses a measure to meet the detection requirement in B.1, it can choose an Intrusion Detection System (IDS), Closed Circuit Television (CCTV) system, or employees or onsite security personnel to provide detection. Furthermore, as opposed to requiring that a facility use a very specific IDS, DHS simply requires that the IDS have one or more of the following types of sensors: infrared (IR) sensors, microwave sensors, fiber-optic sensors, buried cable, magnetic switches, balanced magnetic switches, volumetric motion sensors, glass-breakage sensors, and passive IR motion sensors. See B.1.1. This permits a facility to include a multitude of different non-material deviations in its SSP to address detection, while continuing to comply with the required security measures. A facility is not required to provide a justification for non-material deviations, because these types of deviations are accounted for within the parameters of the required security measures in the guidance.

Based on the above analysis, DHS considers a deviation outside of the parameters set forth in the required risk-based performance measures under CFATS to be a material deviation, and therefore, must be identified and included in the explanation for how the security measure meets the RBPS (as required by section 622(c)(4)(B)(ii)). In determining whether a material deviation is sufficient to meet the relevant portions of all applicable RBPS, the material deviation will be evaluated against the security measures required by this guidance.

Planned Measures

The security measures within the Expedited Approval SSP must either be existing security measures or planned measures with a clear timeline for implementation not to exceed twelve (12) months from date of the approval. See 6 U.S.C. § 622(c)(4)(C)(v). DHS has identified twelve

(12) months as a reasonable time period[3] for planned measures in order to allow for the basic tasks for security system and procedural implementation to include planning and assessment of requirements; design and development of proposed solutions; soliciting bids and identifying/acquiring funding (when required); and installing, testing, and implementing the systems or procedures. This timeframe allows for the appropriate planning and budgeting, while also ensuring expedited completion of planned measures. If a facility cannot implement a planned measure within twelve (12) months, that is a material deviation from this guidance and must be identified within the SSP with details justifying why the 12-month timeframe cannot be met and what timeframe the facility proposes and how the deviation still accomplishes the RBPS. Any item identified as a planned measure must include all relevant details outlining how the planned measure meets the specific guidance.

Other Guidance Requirements

Along with the SSP, the facility must submit a certification, signed under penalty of perjury that meets the requirements of 6 U.S.C. § 622(c)(4)(C). See Attachment 1.

An example of how this guidance can be applied to develop an Expedited Approval SSP is included in Attachment 2. That example identifies how facilities submitting under the Expedited Approval Program may choose to develop their SSP.

Note that in accordance with 6 U.S.C. § 622(c)(4)(G)(ii), if during or after a compliance inspection, the Department of Homeland Security determines that planned or implemented measures in an SSP submitted through the Expedited Approval Program "are insufficient to meet the risk-based performance standards based on a misrepresentation, omission, or inadequate description of the site," DHS may require additional measures or suspend the certification of the facility.

The SSP developed pursuant to this program, as well as certain information exchanged between the facility and DHS staff and/or inspectors during the review process, is considered to constitute Chemical-terrorism Vulnerability Information (CVI) under the CFATS rule and may be shared only with those who have a need to know and have been certified by DHS as authorized users of CVI (see 6 CFR § 27.400 and 6 U.S.C. § 623).

[3] The Act requires facilities submitting under the expedited approval program to implement planned measures within a reasonable time period, which must be stated in the SSP. DHS has identified twelve (12) months as a reasonable time period, which is consistent with the application of the CFATS regulation thus far and is based on best practices and lessons learned in working with the regulated community on the development and implementation of planned measures.

Definitions

Asset: Any on-site or off-site activities; process(es); systems; subsystems; buildings or infrastructure; rooms; capacities; capabilities; 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 chemicals of interest (COI).[4]

Asset-based Security Program: A layered security approach that employs heightened security measures around higher tiered assets.

Certification: A document that is signed under penalty of perjury by the owner or operator of an expedited approval facility and submitted with an Expedited Approval Program SSP that certifies compliance with all of the requirements contained in 6 U.S.C. § 622(c)(4)(C).

Critical Asset: An asset whose theft, loss, damage, disruption, or degradation would result in significant adverse impacts to human life or health.[5]

Critical Cyber Asset: Cyber systems 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 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.[6]

Existing Measure: Security measures that are in place at the time of SSP submission and are assessed by the Department for the purpose of determining whether a facility's SSP satisfies an applicable RBPS.

Operator: A person who has responsibility for the daily operations of a facility or facilities subject to part 27 of title 6 of the Code of Federal Regulations.[7]

Owner: A person or entity that owns any facility subject to part 27 of title 6 of the Code of Federal Regulations.[8]

---

[4] See Department of Homeland Security, Chemical Facility Anti-Terrorism Standards Risk-Based Performance Standards Guidance (May 2009), at 16, *available at* http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

[5] See RBPS Guidance Document at 16.

[6] See RBPS Guidance Document at 71.

[7] See 6 C.F.R § 27.105

Planned Measure: Security measures that are in the process of being implemented by a facility and that can be assessed by the Department for the purpose of determining whether a facility's SSP satisfies an applicable RBPS. These may include security measures that are in the design phase, but have an approved and documented capital budget; are in the bid process and have been placed for bid or for which bids have been received and are under review; are in a pilot phase or in execution as a demonstration project, and for which there is a documented implementation budget and schedule.[9]

Restricted Area: 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.[10]

[8] See 6 C.F.R § 27.105.
[9] See Department of Homeland Security, CFATS Knowledge Center, FAQ 1659 (Jan. 7, 2010), *available at* http://csat-help.dhs.gov.
[10] See RBPS Guidance Document at 16.

Section A: General Facility Information

A facility's security plan submitted under the Expedited Approval Program must include a section on general facility information in order to provide DHS with an accurate picture of the facility's general layout and posture. The information required below should also be validated to be consistent with the information currently in CSAT. This section must include basic facility detail to include at a minimum: the facility name, CSAT Facility ID number, owner/operator, facility address, and facility latitude and longitude, as further described below.

A.1 Facility Owner

The facility must list the names of both the owner and operator as defined in this guidance and 6 CFR § 27.105. The facility must also list the Facility Name as listed within CSAT.

A.2 Facility Location

The facility's address must be its physical location including the street number, street, city, state, and ZIP code. This must include local street and road designations and the address may not include post office box numbers or rural box numbers. The facility must also list its latitude and longitude.

Enter the latitude and longitude of the geographical center of a facility in decimal units with four to six significant digits after the decimal point (e.g., 12.345678). In the United States, latitude is expressed as a positive number, longitude as a negative number. Enter latitude with no sign before it and longitude with a negative sign with no space before the coordinate (e.g., -98.765432). Enter only numeric data.

There are several publicly available tools to help find the latitude and longitude of a facility, such as mapping and aerial photography tools (e.g., Google Earth, TerraServer). To find the geographic center of a facility, use an online map or aerial photography tool and select the approximate geographic center as the point of reference for the latitude and longitude. For additional assistance in identifying the latitude and longitude, see Frequently Asked Question 1560 on the CFATS Knowledge Center (http://csat-help.dhs.gov).

A.3 Facility Type

A brief facility type description must be included. The type must describe the primary purpose of the facility, which may be one of the following:

Agricultural Chemicals Distribution
Agricultural Chemicals Manufacturing
Agricultural Products Processing
Chemical Distribution
Chemical Manufacturing
College/University
Food Distribution
Food Processing
Health Care
Mineral Extraction/Processing
Natural Gas Storage/Transfer
Petroleum Products Distribution
Petroleum Refining
Pharmaceutical Manufacturing
Power Generation
Propane Distribution
Research
Waste Management
Other

If a facility chooses other, the facility must describe the facility type.

A.4 Facility Co-Location

If the facility is a co-located host or tenant, this information and the facility(s) with which the facility shares property must be clearly identified. A facility that is co-located shares a site with another company's facility through either a host or tenant agreement. A facility that does not share a site with another facility must list that it is a sole tenant or that it is not co-located.

A.5 Facility Personnel

The general facility information must also include a list of names and/or titles and contact information of facility personnel with security responsibilities, to include, where applicable the Site Security Officer (SSO), Alternate SSO, Corporate Security Officer, Cyber Security Officer, and Corporate Cyber Security Officer.

The number of facility personnel (broken out for each category of full time, part time, full time contractor, part time contractor, and on-site security) as well as the work shifts and operational coverage must be detailed within the security plan. A facility that is operational 24/7 or has on-site security 24/7 must clearly identify this coverage. Shift hours must indicate the start time and end time for each group's shift.

A.6 Local First Responders

The facility's local Fire Department and Local Law Enforcement office, along with any other applicable local first responders, must be included along with their contact information.

A.7 Chemicals of Interest

Finally, the facility must clearly identify all regulated chemicals of interest (COI) defined in the final tiering letter from DHS and critical assets. For each such COI, the security plan must identify the chemical name, final tier level, security concern/issue (i.e., Theft/Diversion, Release-Toxic, Release-Flammable, Release-Explosive, and Sabotage/Contamination), portability (i.e., man-portable, mechanically portable, bulk storage, or bulk transportation), container type (e.g., railcar, cylinder, tote, bag), and whether the facility receives, manufactures, ships and/or sells the COI. Each critical asset must be listed with an asset name and description. The asset description must include the location of the asset, primary function, COI associated with the asset, and any other information the facility deems necessary to assist DHS in understanding the security posture of the assets.

A.8 Attachments

The facility must upload a plot plan, facility schematic, or similar attachment demonstrating the location of the COI within the facility along with its security plan. To the best extent possible, this attachment should be to scale and detail all avenues of approach, access points, and barriers at the facility.

Section B: Detection Measures

(RBPS 1, 2, 3, 4, 5, 6, and 7)

Background on Detection

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. 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. A facility that has multiple layers of robust delay measures may implement a lower level of detection and still have a successful protection system in place. This must be balanced and described in the SSP and in accordance with the below requirements.

B.1 Detection (RBPS 1, 2, 4, 6 and 7):

Detection must be accomplished through systems, personnel, or a combination thereof and must be located at the critical asset(s), perimeter, or both as further described below. In order to meet the requirement for RBPS for detection, an Expedited Approval Facility must include in its plan one or more of the following in accordance with the requirements below:

- Intrusion Detection System (IDS)
- Closed Circuit Television (CCTV) system
- Employees or onsite security personnel

B.1.1 If a facility utilizes an Intrusion Detection System (IDS), it must:

B.1.1.1 Include one or more of the following types of sensors and deploy in accordance with the manufacturer's specifications: infrared (IR) sensors, microwave sensors, fiber-optic sensors, buried cable, magnetic switches, balanced magnetic switches, volumetric motion sensors, glass-breakage sensors, and passive IR motion sensors.

- When utilizing exterior sensors such as IR, microwave, fiber-optic, or buried cable, facilities must take into account weather and terrain to ensure effective deployment of sensors.
- When using IR or passive IR, the IR energy must be focused onto the targeted area for detection.
- When utilizing a magnetic switch or balanced magnetic switch, facilities must mount the mechanism on the doorframe or window frame and the actuating magnet on the door or window.

B.1.1.2 Be activated at all times when another detection method identified within this document (see B.1.2 and B.1.3) is not available.

B.1.1.3 Cover either all perimeter entry point(s) (doors and windows, as applicable) or all access point(s) leading to the critical asset(s).

B.1.1.4 Alarm to a responsible and trained individual(s) to initiate a response either through local alarm, central station, auxiliary connection (police or fire), or proprietary station.

- When a sensor or other IDS component identifies an event of interest, an alarm must notify facility management, security personnel, local law enforcement, or a third party who then must assess the event either directly by sending one or more persons to the location of the event or remotely by alerting personnel to evaluate sensor inputs and surveillance imagery.
- If the facility uses a third party company or facility personnel who dispatch personnel, the IDS must alarm to individuals who are trained to ensure that appropriate law enforcement or other security responders are dispatched and that a facility point of contact is reached.

B.1.1.5 Include back-up power or deploy personnel as described below to provide detection during system outages or failures.

- If back-up power is utilized it must:
  - Start automatically upon failure of the primary power;
  - Be adequate to power the required systems for at least an amount of time (which must be stated in the SSP) which facility officials believe is sufficient for power to be restored after an outage;
  - Be equipped with adequate fuel supply to last for at least the amount of time described in the previous bullet;
  - Be tested to ensure efficiency and effectiveness; and
  - Be located in a restricted area for added security.

- If the facility deploys personnel as a compensatory measure for system failures or outages, they must:
  - Be deployed immediately upon notification of the outage and in place within one hour of failure/outage notification;
  - Remain in place until the failure or outage is resolved; and
  - Be trained and capable to provide detection at all perimeter entry point(s) (doors and windows, as applicable) or all access point(s) leading to the critical asset(s) where system failures have occurred during this time (see B.1.3).

If a facility elects to use IDS to satisfy B.1, material deviations from this guidance include any measure that does not meet the specific requirements contained in B.1.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes monitoring of perimeter and critical asset(s) comparable to the requirements in B.1.1 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), RBPS 4 (detect breach of the perimeter/critical assets), RBPS 6 (deter theft and diversion through perimeter/critical asset monitoring), and RBPS 7 (deter insider sabotage through perimeter/critical asset monitoring). For example, a measure that compensates for system outages or failures in a manner not described above is a material deviation from B.1.1.

B.1.2 If a facility utilizes a Closed Circuit Television (CCTV) system, it must:

B.1.2.1 Include the integration of cameras, recorders, switches, keyboards, and monitors.

B.1.2.2 Ensure the capability to detect an object, recognize the type of object, and identify the details of the object and be deployed in accordance with manufacturer's specifications.

B.1.2.3 Be activated at all times when another detection method (see B.1.1 and B.1.3) is not available.

B.1.2.4 Cover all perimeter entry point(s) (doors and windows, as applicable), all critical asset(s) access point(s), or all critical asset(s) area(s).

B.1.2.5 Have appropriate security lighting (see B.2.1).

B.1.2.6 Be monitored by a dedicated and trained individual(s) or be equipped with motion detection to alarm to a responsible and trained individual(s) to initiate a response.

- When the CCTV system relies on motion detection which alarms to an individual, the video-processing system must be linked to communicate to the alarm-processing system.

B.1.2.7 Include back-up power or deploy personnel as described above (see B.1.1) to provide detection during system outages or failures.

B.1.2.8 Include information transmission via one of the following methods: metallic video cables, RF transmission, and/or fiber-optic cable.

If a facility elects to use CCTV to satisfy B.1, material deviations from this guidance include any measure that does not meet the specific requirements contained in B.1.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the monitoring (perimeter and critical asset(s)) comparable to the requirements in B.1.2 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), RBPS 4 (detect breach of the perimeter/critical assets), RBPS 6 (deter theft and diversion through perimeter/critical asset monitoring, and RBPS 7 (deter insider sabotage through perimeter/critical asset monitoring). For example, such deviations include implementing a compensatory measure for system outages or failures which is not described above.

B.1.3 If the facility utilizes employees or on-site security personnel, they must:

B.1.3.1 Be capable of providing and trained to provide detection of an intrusion or attempted theft as further described below; and

B.1.3.2 Be either dedicated to perimeter access point(s), critical asset(s) access point(s), or critical asset(s) area(s) or conduct roving patrols of the perimeter or critical asset(s) area(s).

Being capable of providing detection includes having the time, resources, proper security lighting (see B.2.1), and viewpoint to provide the detection. Being trained to provide detection requires training which must include:

- Identifying attempts to breach the access point(s) or area(s);

- Recognizing suspicious persons or vehicles;
- Identifying degradation to security measures (barriers, locks, etc.),
- Detecting inventory control issues; and
- Reporting (how and to whom) these potential security incidents.

If a facility elects to use employees or security personnel to satisfy B.1, material deviations from this guidance include any measure that does not meet the specific requirements in B.1.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes monitoring (perimeter and critical asset(s)) comparable to the requirements of B.1.3 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), RBPS 4 (detect breach of the perimeter/critical assets), RBPS 6 (deter theft and diversion through perimeter/critical asset monitoring, and RBPS 7 (deter insider sabotage through perimeter/critical asset monitoring).

B.1.4 Tier 3 and 4 facilities which choose to participate in the Expedited Approval Program must ensure a detection capability which creates sufficient time to allow for a response between the detection of an attack and the point at which the attack becomes successful. The point at which an attack becomes successful is closely linked to the type of attack being attempted and the event that is meant to be caused. This is most clearly identified by the facility's regulated COI and security concern(s) (Theft/Diversion, Release, and Sabotage).

A **Theft/Diversion** attack becomes successful when the COI is successfully taken off-site or diverted either through theft or deception and utilized in a terrorist attack. Therefore, a detection capability for these facilities must be able to detect the action prior to this success either upon attempt to gain access to the facility, depart with the COI, or utilize the COI in the attack. Facilities tiered for **Theft/Diversion** must accomplish detection through any of or a combination of the methods identified above.

A **Release** attack becomes successful instantly at the point of the attack and therefore the facility must provide continuous monitoring in order to detect the attempted attack when it becomes imminent. Facilities tiered for **Release** must accomplish detection through any of or a combination of the methods identified above.

A **Sabotage** attack becomes successful offsite after allowing an on-site tampering; therefore, the facility must provide continuous monitoring through any of or a combination of the methods identified above or monitoring via one of the methods identified in B.1.4.3.

B.1.4.1 Facilities tiered for **Theft/Diversion** must ensure there are gaps in detection no greater than four (4) hours commensurate with the level of delay. If a facility is able to create a robust delay capability (see C.1.1.3), the facility must ensure that there are gaps in detection no more than eight (8) hours. This ensures that detection is likely to occur prior to the attempt, at the moment of the attempt, or at a minimum of prior to successful utilization of the COI for the attack.

With regard to B.1.4.1, material deviations from this guidance include any measure that does not meet the specific requirements contained in B.1.4.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the monitoring comparable to the requirements in B.1.4.1 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), RBPS 4 (detect breach of the perimeter/critical assets), and RBPS 6 (deter theft and diversion through perimeter/critical asset monitoring). For example, material deviations from this guidance include a monitoring capability with gaps greater than eight (8) hours with mitigating factors such as added delay.

B.1.4.2 Facilities tiered for **Release** must ensure continuous monitoring through dedicated sources. This cannot allow for any breaks in detection.

With regard to B.1.4.2, material deviations from this guidance include any measure that does not meet the specific requirements contained in B.1.4.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the monitoring comparable to the requirements in B.1.4.2 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), and RBPS 4 (detect breach of the perimeter/critical assets). For example, material deviations from B.1.4.2 include less than continuous monitoring capability with mitigating factors such as containment vessels, fire suppression systems, or other process safeguards, and detection via other means than those described above such as via leak detection systems, gas alarm, process alarm, etc.

B.1.4.3 Facilities tiered for **Sabotage** must perform detection through one or more of the following:

- Continuous monitoring through dedicated sources via one of the methods described above;

- 100% screening and inspections for contraband upon entering the facility or critical asset(s) area(s) (see C.3.3 and C.3.4); or
- Shipping procedures requiring 100% inspection of shipments and tamper evident devices upon egress (see C.5.8).

With regard to B.1.4.3, material deviations from this guidance include any measure that does not meet the specific requirements in B.1.4.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the monitoring comparable to the requirements in B.1.4.3 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), RBPS 4 (detect breach of the perimeter/critical assets), RBPS 6 (deter theft and diversion through perimeter/critical asset monitoring, and RBPS 7 (deter insider sabotage through perimeter/critical asset monitoring).

B.2 Security Lighting (RBPS 1, 2, and 4):

Security lighting can help to both deter attempts at penetrating a facility's perimeter and assist in the monitoring and detection of any such attempts. Due to the increased likelihood of detection based on appropriate security lighting, maintaining a well-lit facility perimeter also can help deter adversaries from attempting to breach that perimeter.

B.2.1 Facilities must provide and maintain sufficient illumination levels (at a minimum of 5 foot-candles for indoor storage areas and 10 foot-candles for outdoor storage areas) to permit individual(s) to perform their duties, provide appropriate surveillance, and properly utilize all security equipment (e.g., CCTV systems).

With regard to B.2.1, material deviations from this guidance include any measure that does not meet the specific requirements in B.2.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes security lighting comparable to the requirements of B.2.1 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (monitor the perimeter), RBPS 2 (monitor restricted areas and potentially critical targets), and RBPS 4 (detect breach of the perimeter/critical assets). For example, material deviations from B.2.1 include deploying security lighting in a manner that is inconsistent with the above.

B.3 Inventory Control (RBPS 5 and 6):

All facilities must have proper inventory management. Proper inventory management includes the following:

B.3.1 Written inventory procedures must be developed. These must require that at least one person be responsible for conducting inventories and outline the roles and responsibilities of individuals charged with conducting inventories. This must also outline the processes for how the facility conducts inventory. The procedures must include maintaining records, either in the form of logs, charts, or electronic systems. The records must be capable of demonstrating that the inventories have been conducted and when and by whom.

B.3.2 Facilities must achieve regular and recurring inventories through one of the below:

- Process control systems that monitor the level, weight, and/or volume of the COI continuously; or
- Weekly (at a minimum) COI inventory checks (e.g., cycle counts) by an individual charged with maintaining and recording inventory.

With regard to B.3, material deviations from this guidance include any measure that does not meet the specific requirements contained in B.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the inventory comparable to the requirements in B.3 and how the measure accomplishes sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 5 (monitor the shipping of hazardous materials and RBPS 6 (deter theft and diversion of potentially dangerous chemicals). For example, material deviations from this guidance include conducting inventory via a method not described above.

Section C: Delay Measures (RBPS 1, 2, 3, 4, 5, 6, and 7)

Background on Delay

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. 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://csat-help.dhs.gov/). As described in Section A.7, facilities must clearly identify and describe all COI and critical assets in order to justify taking an asset-based approach versus a facility-wide approach.

C.1 Human Barriers (RBPS 1, 2, 4, 6 and 7):

Barriers provide both physical obstacles and psychological deterrents to unauthorized entry, thereby delaying or preventing forced entry.

C.1.1 To achieve appropriate delay measures, facilities must utilize barriers which completely enclose the perimeter or critical asset(s) utilizing walls or security fences. A facility's SSP must explain how the facility perimeter or critical assets(s) are completely enclosed using fences and/or walls.

C.1.1.1 When choosing to utilize fencing, it must be constructed of chain-link, barbed wire, or concertina and must be a minimum of seven (7) feet high (including topper, where applicable).

Chain-link fences must be constructed with nine (9) gauge or heavier wire and have openings not larger than two (2) inches per side. The fencing must be stretched and fastened to metal posts and must reach within two (2) inches of the ground or pavement in order to further delay an intruder crawling under or lifting up the fence. To protect the fence from washouts or channeling under, culverts or troughs should be provided at natural drainage points. Any such openings larger than 96 square inches must be provided additional physical barriers to limit access.

Barbed wire fences must be constructed of 13.5-gauge twisted double strand wire with four (4) point barbs no more than four (4) inches apart. These must be placed on metal posts no more than six (6) feet apart.

Concertina wire can be used with one roll atop another or in a pyramid with two rolls along the bottom and one roll along the top. Ends must be fastened together and secured to the ground.

C.1.1.2 When utilizing walls as barriers, they must be constructed of brick, cinder block, poured concrete, wood, or metal panel and must be a minimum of seven (7) feet high (including topper, where applicable).

C.1.1.3 Facilities tiered for Theft/Diversion COI may decide to create a more robust delay capability in order to reduce the necessary detection requirement from every four (4) hours to every eight (8) hours (see B.1.4.1). In order to justify a reduced detection capability, facilities must have at least two layers of barriers enclosing the facility or all critical asset(s), one of which is made of walls constructed of brick, cinder block, poured concrete, wood, or metal panel.

With regard to C.1.1, material deviations from this guidance include any measure that does not meet the specific requirements contained in C.1.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation of how the deviation accomplishes the delay comparable to the requirements of C.1.1 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (secure the perimeter), RBPS 2 (secure restricted areas and potentially critical targets), RBPS 4 (delay an attack for a sufficient period of time to allow appropriate response), RBPS 6 (deter theft and diversion through securing perimeter/critical asset, and RBPS 7 (deter insider sabotage through securing perimeter/critical asset). For example, such deviations include implementing barriers which do not completely enclose the perimeter or critical asset(s).

C.1.2 All facilities must also utilize locking mechanisms for entry points to all perimeter or all critical asset(s) which must be of one or more types: locksets, deadbolts, magnetic locks, padlocks, cam locks, mortise locks, and/or cylinder locks. Access points must remain locked at all times when access point is not in use or manned. This must take into account mechanisms associated with fire safety.

With regard to C.1.2, material deviations from this guidance include any measure that does not meet the specific requirements contained in C.1.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation of how the deviation accomplishes the delay comparable to the requirements of C.1.2 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (secure the perimeter), RBPS

2 (secure restricted areas and potentially critical targets), RBPS 4 (delay an attack for a sufficient period of time to allow appropriate response), RBPS 6 (deter theft and diversion through securing perimeter/critical asset, and RBPS 7 (deter insider sabotage through securing perimeter/critical asset). For example, such deviations include: implementing locks which do not cover all entry points to the perimeter or all critical asset(s), and utilizing a lock not described above.

C.1.3 If facilities use keys/locks, combinations, and/or access credentials, they must maintain a key/lock, combination, and/or access credential control and accountability program which ensures keys, locks, combinations, and access credentials are only issued to authorized individuals, are collected upon termination of employment or change in work status, are periodically inventoried, and are changed when there is a loss or suspicion of compromise or upon termination of employment.

A periodic inventory of keys, combinations, and/or access controls must be conducted at a minimum of annually.

With regard to C.1.3, material deviations from this guidance include any measure that does not meet the specific requirements contained in C.1.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the delay comparable to the requirements of C.1.3 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 4 (deter attacks through visible, professional, well-maintained security measures and systems and delay an attack to allow time for an appropriate response). For example, material deviations from this guidance include conducting inventory of keys, combinations, and/or access controls at a frequency less than annually.

C.2 Vehicle Barriers for Release COI (RBPS 1, 2, and 4):

C.2.1 Facilities tiered for Release COI must employ vehicle barriers such as bollards, berms, ditches, revetments, cables, moats, capture nets, and/or jersey barriers at the perimeter or critical asset(s) in order to reduce the likelihood of accessing the facility or critical asset(s) by force or employing a Vehicle-Borne Improvised Explosive Device (VBIED) in close proximity to a Release COI. Vehicle barriers must be deployed in accordance with Unified Facilities Criteria (UFC) 4-010-01 and UFC 4-020-01 and be included on the DOD Anti-Ram Vehicle Barrier List.

With regard to C.2.1, material deviations from this guidance include any measure that does not meet the specific requirements contained in C.2.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this

requires an explanation within the SSP of how the deviation accomplishes the delay comparable to the requirements of C.2.1 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 1 (secure the perimeter), RBPS 2 (secure restricted areas and potentially critical targets), and RBPS 4 (deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets) For example, such deviations include deploying a vehicle barrier in a manner that is inconsistent with the requirements of UFC 4-010-01 and UFC 4-020-01.

C.2.2 Facilities tiered for Release COI must also establish a standoff distance for Release COI assets. Standoff distances must be deployed in accordance with minimum standoff distances established in UFC 4-010-01. Where necessary, standoff distance may be increased to reduce the blast effects on an asset. The required standoff distances will vary with building components used in the construction.

With regard to C.2.2, material deviations from this guidance include any measure that does not meet the specific requirements contained in C.2.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the delay comparable to the requirements of C.2.2 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 4 (deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets and deter attacks through visible, professional, well-maintained security measures and systems). For example, material deviations from the guidance include reduced standoff distance with additional asset hardening, to include additional barriers.

C.3 Access Control (RBPS 3 and 7):

Through access control measures to include identification, screening, and inspection, a facility is better able to prevent unauthorized access to the facility or its restricted areas and is more likely to deter and detect unauthorized introduction or removal of substances and devices that may cause a dangerous chemical reaction, explosion, or hazardous release. Restricting access to only authorized individuals requires personnel identification. Personnel identification measures help a facility quickly determine whether or not an individual is permitted access to a facility or a restricted area, and certain identification measures can help both security officers and other employees quickly know whether or not an individual is authorized for access.

C.3.1 Facilities must establish a personnel identification program. This must include validating the identity of all visitors requesting access to the facility or critical asset(s) via government-issued photo identification (ID) card.

Note: Personnel surety requires four types of background checks for unescorted visitors (see F.3). The above refers to all visitors regardless of access levels.

To further accomplish personnel identification, facilities must implement one or more of the following for all facility personnel, contractors and visitors.

C.3.1.1 Permitting facility or restricted area access only to those on approved entry lists and conducting checks of government-issued photo ID cards to verify that entering employees, contractors or visitors are on the lists.

C.3.1.2 Providing company-issued, facility-specific photo IDs, or access credentials to individuals permitted access to the facility or restricted areas of the facility. Photo identifications should identify whether the individuals have access to restricted areas and also should identify whether the individuals are:

- Employees,
- Regular contractors,
- Temporary contractors, or
- Visitors.

Photo ID cards or similar unique identifiers (e.g., key fobs, access, codes) may be linked with electronic access control systems, such as proximity ID readers or swipe-access controls for an added layer of security. 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.

C.3.1.3 Utilizing employee training to recognize and identify facility personnel granted access. Note: This method is only appropriate for a small workforce, 50 personnel per shift or less, where manual personnel identification can be accomplished.

With regard to C.3.1, material deviations from the guidance include any measure that does not meet the specific requirements contained in C.3.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the access control comparable to the requirements of C.3.1 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 3 (control access to the facility and to restricted areas) and RBPS 7 (deter insider sabotage through access controls and screening). For example, such deviations include utilizing a different method

of personnel identification rather than company-issued, facility-specific photo IDs, or access credential.

C.3.2 Facilities must restrict access within the perimeter or restricted area(s) to only authorized individuals by one or more of the below means. This includes ensuring individuals are authorized through verifying the completion of background checks required under F.3.

C.3.2.1 An electronic access control system (ACS). Electronic ACS consist of electronic locks, card readers, biometric readers, alarms (where applicable), and computer systems to monitor and control access. If choosing to implement access control via an ACS, facilities must utilize credential devices, coded devices, or biometric devices and must implement them in accordance with manufacturer's specifications.

C.3.2.2 Physical locking mechanisms. Physical locking mechanisms are identified above under C.1.2.

C.3.2.3 Implementation by facility personnel (e.g., security guards or supervisors) of screening and inspection procedures, as further described in Sections C.3.3 and C.3.4.

With regard to C.3.2, material deviations from the guidance include any measure that does not meet the specific requirements contained in C.3.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the access control comparable to the requirements of C.3.2 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 3 (control access to the facility and to restricted areas) and RBPS 7 (deter insider sabotage through access controls and screening).

C.3.3 For **Release** and **Sabotage facilities,** inspection of items brought into the facility or restricted area(s) of the facility must be done in one or more of the following ways, focusing on screening for firearms, explosives, or materials which could alter the security of Release and/or Sabotage assets:

- Visual inspections, which include the examination of the contents of any item brought into the facility,
- X-ray inspections,
- Use of metal detectors,
- Use of ionic explosives detection equipment, or
- Use of trained explosive detection dog team.

With regard to C.3.3, material deviations from the guidance include a measure does not meet the specific requirements contained in C.3.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the access control comparable to the requirements of C.3.3 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 3 (control access to the facility and to restricted areas) and RBPS 7 (deter insider sabotage through access controls and screening).

C.3.4 Facilities tiered for **Release** COI must conduct screening and inspections of vehicles prior to allowing vehicle access to the perimeter and/or Release critical asset(s) in one or more of the following ways, focusing on screening for firearms, explosives, or materials which could alter the security of release assets:

- Visual inspections,
- Use of trained explosive detection dog team,
- Under/over vehicle inspection systems, or
- Cargo inspection systems.

During these inspections, drivers and passengers should remain with vehicles and the individual performing the inspections must conduct a thorough and systematic search of the vehicles to include the vehicle exterior, interior, trunk, cargo, and other compartments.

With regard to C.3.4, material deviations from the guidance include any measure that does not meet the specific requirements contained in C.3.4. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the access control comparable to the requirements of C.3.4 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 3 (control access to the facility and to restricted areas). For example, material deviations from the guidance include conducting screening or inspections to less than all vehicles prior to allowing access to critical asset(s) or in a manner inconsistent with the above.

C.4 Receiving Procedures (RBPS 5 and 6):

Facilities which receive COI must:

C.4.1 Plan in advance all in-bound shipments of COI.

C.4.2 Ensure COI is being received from a known and prior-approved shipper.

C.4.3 Inspect trucks, trailers, and rail cars, where applicable, upon entering the facility or restricted area(s).

Incoming trucks, trails, and rail cars to the facility must be inspected. If a cargo or rail car is sealed, the seal must be checked and verified. If the seal has been tampered with or broken, it must be reported. Inspections must be in accordance with vehicle inspections guidance within Section C.3.4.

C.4.4 Transfer COI from unloading areas to storage or process areas in an expeditious manner in order to ensure the COI is not left unattended in the unloading area. COI must be attended at all times by a facility employee with authorized access while in unsecured areas. Receiving and unloading procedures must ensure that COI are moved from unloading areas to storage or processing areas without being left unattended.

This includes coordinating effective business relationships and having procedures for handling the arrival of an unknown carrier at the facility, including the staging of a vehicle and its driver until both the driver and the load are vetted and approved.

For facilities that do not receive COI, this must be noted in the SSP.

With regard to C.4, material deviations from the guidance include any measure that does not meet the specific requirements contained in each of the measures in C.4. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the security comparable to the requirements of C.4 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 5 (monitor the receipt of hazardous materials for the facility).

C.5 Shipping Procedures (RBPS 5, 6, and 7):

Facilities that ship or sell COI must:

C.5.1 Plan and approve all shipments of COI in advance using known and prior-approved, carriers.

C.5.2 Have procedures or practices to ensure multiple levels of review and validation of all shipments.

C.5.3 Have a Know Your Customer program or similar practice which ensures customers of COI are properly vetted to include verifying a customer's identity, business location, financial status, and COI end use.

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

- 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.

C.5.4 Have a procedure or practice to refuse the sale of COI unless customers meet customer vetting and identification procedures.

C.5.5 Establish normal business-to-business payment terms and methods that prevent cash sales to customers.

C.5.6 Ensure all sales and shipments of COI are documented including, the method of shipment, carrier information, the times and dates of shipments, and the destination. The records must be maintained a minimum of three years.

C.5.7 Utilize tamper-evident mechanisms to identify tampering with COI prior to and during shipment.

C.5.8 Inspect trucks, trailers, and/or rail cars, where applicable, prior to loading and departing.

Incoming and outgoing trucks, trails, and rail cars to the facility must be inspected. If a cargo or rail car is sealed, the seal must be checked and verified. If the seal has been tampered with or broken, it must be reported. Inspections must be in accordance with vehicle inspections guidance within C.3.4.

C.5.9 Confirm all shipments have arrived at their final destination.

C.5.10 Ensure systems are in place to track and protect shipments en route to their destinations, such as driver call-in schedules, GPS tracking, etc.

Facilities that do not ship or sell COI must document within the SSP that they do not ship or sell the COI.

With regard to C.5, material deviations from this guidance include any measure that does not meet the specific requirements contained in each of the measures in C.5. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the security comparable to the requirements of C.5 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 5 (monitor the shipping of hazardous materials for the facility), RBPS 6 (deter the diversion of potentially dangerous chemicals), and RBPS 7 (deter insider sabotage through shipping procedures).

Section D: Response Measures (RBPS 9, 11, 13, and 14)

Background on Response

Response within this 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 COI. This includes plans to mitigate and/or respond to the consequences of a security incident and to report security incidents internally and externally in a timely manner. An appropriate response must 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 must address the identification of the hazards and the equivalent response plans. Response plans must identify the number and capabilities of the various responders, and the equipping and training of response personnel. Properly equipped personnel, who understand the potential consequences of a security incident and the need for timely, effective actions, when coupled with well-rehearsed response plans, reduce the probability of an attack achieving the adversaries' desired goals. Additionally, practiced response plans help ensure that on-site responders and emergency-response units from local law enforcement, firefighting, ambulance, mutual aid, and rescue agencies are familiar with the facility and chemicals stored on site and are not impeded from reaching the location of the security event.

D.1 Response Planning (RBPS 9 and 11)

D.1.1 Facilities must have a defined emergency and security response organization in order to respond to site emergencies and security incidents.

Facilities with less than 100 employees may utilize a single security official. Facilities with more than 100 employees must identify two or more security officials. Regardless of the size of the security organization**,** it must include coordination with local first responders.

With regard to D.1.1, material deviations from this guidance would include any measure that does not meet the specific requirements contained in D.1.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the security comparable to the requirements of D.1.1 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 9 (develop an emergency plan to respond to security incidents).

D.1.2 In order to conduct proper response planning, the facility must have a crisis management plan, which includes at a minimum:

- Emergency response procedures;
- Security response plans; and
- Post-incident security plans (post-terrorist attack, security incident, natural disaster, etc.).

All three of the above plans and procedures must specifically address the COI, security concern, and associated attack scenarios. Facilities may also choose to include other elements in these plans, such as:

- Contingency plans,
- Continuity of operations plans,
- Notification control and contact requirements, and
- Re-entry plans.

D.1.2.1 Facilities tiered for **Release** COI must have additional portions to their crisis management plan, which 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.

With regard to D.1.2, material deviations from this guidance include any measure that does not meet the specific requirements contained in D.1.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation meets the security comparable to the requirements of D.1.2 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 9 (develop an emergency plan to respond to security incidents).

D.1.3 The facility must have designated individual(s) responsible for executing each portion of the crisis management plan and these individual(s) must be trained to execute all duties.

With regard to D.1.3, material deviations from this guidance include any measure that does not meet the specific requirements contained in D.1.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the security comparable to the requirements of D.1.3 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 9 (develop and exercise an emergency plan to respond to security incidents) and RBPS 11 (ensure proper security training, exercises, and drills of facility personnel). For example, material deviations from this guidance include training only employees within specific areas or functions of the facility.

D.1.4 The facility must have the appropriate resources (e.g., staff, emergency/response equipment, building space, communications equipment, process controls/safeguards) to execute all response plans. These resources must be identified in the crisis management plan.

Emergency equipment must include all equipment identified within the response plans, which must include at least one of the following:

- A radio system that is redundant and interoperable with law enforcement and emergency response agencies.
- At least one backup communications system, such as cell phones/desk phones.
- An emergency notification system (e.g., a siren or other facility-wide alarm system).
- Automated control systems or other process safeguards for all process units to rapidly place critical asset(s) in a safe and stable condition and procedures for their use in an emergency.
- Emergency safe-shutdown procedures for all process units.

These plans must be developed along with or shared with local law enforcement and appropriate first responders (see D.1.6).

With regard to D.1.4, material deviations from this guidance include any measure that does not meet the specific requirements contained in D.1.4. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation meets the comparable security as required within D.1.4 and how the measure accomplishes sufficient security required within relevant portions of RBPS 9 (develop and exercise an emergency plan to respond to security incidents internally). For example, material deviations from this guidance include utilizing outside resources in order to execute response plans.

D.1.5 Facilities must ensure that all facility personnel have been trained on all response plans (see F.2) and must exercise these plans on a regular basis and at a minimum of biennially with employees and others with security responsibilities.

With regard to D.1.5, material deviations from this guidance include any measure that does not meet the specific requirements contained in D.1.5. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the comparable training as required within D.1.5 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 9 (develop and exercise an emergency plan to respond to security incidents) and RBPS 11 (ensure proper security training, exercises, and drills of facility personnel). For example, material deviations from this guidance include training only employees within specific areas or functions of the facility.

D.1.6 In order to ensure that external resources are properly prepared, the facility must have an active outreach program with local first responders (including, but not limited to, the local Police Department and Fire Department). The outreach program must include:

- Providing response and safety documentation to local first responders,
- Providing facility layout information to local first responders,
- Inviting local first responders to facility orientation tours,
- Notifying local first responders of the facility's COI (regulated COI and other chemical holdings identified on Appendix A), security concern, and inclusion in CFATS, and
- Maintaining regular communication (at a minimum of annual) with local first responders.

With regard to D.1.6, material deviations from this guidance include any measure that does not meet the specific requirements contained in D.1.6. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements of D.1.6 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 9 (exercise an emergency plan to respond to security incidents with the assistance of local law enforcement and first responders).

D.2 Elevated and Specific Threats (RBPS 13 and 14):

The ability to escalate the levels of security measures for periods of elevated threat provide a facility with the capacity to increase security measures to better protect against known increased threats or generalized increased threat levels declared by the Federal government. DHS utilizes the National Terrorism Advisory System (NTAS) to communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports, and other transportation hubs for the private sector. This system will alert at two different levels, elevated and imminent. Facilities are required to increase their security measures for these levels and when specific threats are identified and reported to them.

D.2.1 Facilities must have a documented process for increasing security measures commensurate to the designated threat level during periods of elevated threats tied to the NTAS and when notified by DHS of a specific threat.

D.2.2 The facility must begin to execute security measures for elevated and specific threats within eight (8) hours of notification.

D.2.3 Measures which should be implemented for elevated or specific threats will depend on the threat and security posture of the facility. At a minimum, facilities must execute the following measures as a result of an elevated or specific threat:

D.2.3.1 Coordinate with federal, state, and/or local law enforcement agencies to identify recommended actions and additional security measures.

D.2.3.2 Increase detection efforts through continuous monitoring of security systems (IDS or CCTV), hourly patrols of the perimeter and/or critical asset area(s), or continuous stationing of personnel at access points and/or critical asset area(s).

D.2.3.3 For **Theft/Diversion** facilities only, 100% screening and inspections of outbound vehicles or containers capable of concealing COI.

D.2.3.4 For **Sabotage** facilities only, 100% inspection of all outbound shipments.

D.2.3.5 For **Release** facilities only, 100% screening and inspections of inbound vehicles.

Facilities may choose to implement additional measures. The following are examples of measures for an elevated threat condition:

- Taking additional security precautions at public events held on-site and possibly considering alternative venues or event cancellation;
- Preparing to execute contingency procedures, such as moving to an alternate facility or dispersing the workforce;
- Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
- Adding additional barriers at vehicle access points and around critical assets and restricted areas to control traffic and increase standoff distances;
- Adding additional illumination for remote areas;
- Decreasing the number of personnel authorized to be on-site;
- Extending physical protection of vulnerable points;
- Increasing frequency of perimeter patrols;
- Increasing security force allocations;
- Increasing rail car inspections;
- Increasing personnel and vehicle screening inspections;
- Requiring mandatory visitor escorts;
- Minimizing the number of gates in use;
- Instituting off-site mail handling;
- Instituting parking restrictions;
- Postponing projects and activities where critical assets are more exposed or vulnerable;

- Instituting real-time reporting capability between the security control center and the main process control center; and
- Reinforcing barriers at remote or unused gates.

The following are examples of measures for imminent threat conditions:

- Increasing or redirecting personnel to address critical emergency needs;
- Decreasing the number of personnel on-site to "essential" personnel only;
- Performing constant perimeter patrols;
- Instituting maximum security force staffing;
- Inspecting 100% of rail cars;
- Performing100% personnel- and vehicle-screening inspections;
- Prohibiting visitors on-site;
- Prohibiting parking on-site (except for vehicles that are always kept inside the restricted area);
- Arranging to have in place a secure, armed-response capability by making use of any combination of proprietary, contract, local, state, and/or Federal resources where safety at the facility is not compromised.

With regard to D.2, material deviations from this guidance include any measure that does not meet the specific requirements contained in each of the measures in D.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the security comparable to the requirements of D.2 and how the measure accomplishes the sufficient security required within the relevant portions of the applicable RBPS, specifically: RBPS 13 (escalate the level of protective measures for periods of elevated threat) and RBPS 14 (address specific threats, vulnerabilities, or risks).

Section E: Cyber Security Measures (RBPS 8)

Background on Cyber Security

In order to meet the intent of RBPS 8, facilities must deter cyber sabotage and minimize the consequences of physical events, including 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. Protecting against adverse cyber events is essential to the management of the overall risk for a facility. Comprehensive cyber security policies, practices and people are required to protect, prevent, mitigate, respond and recover from adverse cyber events.

E.1 Cyber Security – General (RBPS 8):

Cyber systems that a facility must 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 must 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).

When thinking about cyber security as it relates to CFATS, facilities should keep in mind their COI and the specific security issue. The cyber security measures described must address how cyber security systems impact the security of the COI and how they are utilized to protect the critical cyber systems from being utilized to cause a release or divert or steal the COI depending on the respective security issues(s).

E.1.1 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.

If a facility does not have any critical cyber systems, this must be stated in the SSP along with a description of how their cyber systems are not critical, as defined above.

E.1.2 The facility must develop, maintain, and implement documented and distributed cyber security policies and procedures including change management policies, as applicable, to their critical cyber assets. Appropriate cyber security policies must cover all aspects of cyber security measures, as applicable to the facility, and must include at a minimum the following topic areas:

- Access control,
- Password management,
- Physical security to cyber assets and media, and
- Incident reporting.

Change management is a formal process for directing and controlling alterations to the information processing environment. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment. Change management policies must cover account policy mandates, security concerns, business impact, authorization, and oversight. All policies and procedures must be provided to all employees and contractors, as appropriate, who have a potential to impact the security of the critical cyber system.

E.1.3 The facility must designate a trained and qualified individual(s) to manage cyber security for the facility and to provide direction, accountability, and oversight for cyber security controls. A trained and qualified individual must include having the time, resources, and training in order to carry out the required duties to include at a minimum identifying and protecting cyber assets and information, and detecting, responding to, and recovering from cyber security incidents. This requires recurring training (at a minimum of biennially) on topics which must include:

- Access control methods for critical business and control network systems (including remotely operated control system or business systems);
- Personnel security;
- Cyber security controls, monitoring, response, and reporting;
- Disaster recovery and business continuity;
- System development and acquisition; and
- Configuration management and auditing.

E.1.4 The facility must maintain account access control to critical cyber systems utilizing the least privilege concept (i.e., granting people only as much access as they need to perform their assigned job functions) and limit access to systems using limited administrator and user roles and responsibilities.

E.1.5 The facility must maintain access control lists and ensure that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated immediately when personnel leave and when users no longer require access (e.g., when personnel leave the company, complete a transfer into a new role, or their responsibilities change).

E.1.6 The facility must implement password management protocols to enforce password structures, ensure all default passwords have been changed (where possible), and implement physical controls for cyber systems where changing default passwords is not technically feasible.

Physical controls to mitigate default passwords include the delay measures listed within C.1 in order to secure the building, room, access panel, or other element through physical security measures.

E.1.7 The facility must ensure that physical access to critical cyber assets and media is restricted to authorized users and affected individuals (as defined in F.3).

E.1.8 The facility must provide cyber security training to all employees and contractors, as appropriate, who work with critical cyber assets. This includes the development of a cyber security training program, which establishes the types and frequency of training. At a minimum this training must include the following elements on a biennial basis:

- General company policy review;

- Roles and responsibilities;
- Password procedures;
- Acceptable practices / Rules of behavior; and
- Incident reporting procedures.

With regard to E.1.8, material deviations from this guidance include any measure that does not meet the specific requirements contained in E.1.8. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the training comparable to the requirements within E.1.8 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage). For example, material deviations from this guidance include conducting cyber security training for only a selection of employees or conducting training which is inconsistent with the above.

E.1.9 The facility must report significant cyber incidents to senior management and DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (https://ics-cert.us-cert.gov/) according to reporting timeframes as defined in US-CERT's Federal Agency Incident Categories. Significant cyber incidents are those incidents with malicious intent to adversely affect operations of critical cyber assets, including IT equipment used to provide security for the facility, manage processes involving the COI, or manage critical assets of the facility. In order to ensure proper reporting, facilities must have a documented process for the identification and reporting of significant cyber incidents and must provide awareness and training to employees to carry out this function.

With regard to E.1, material deviations from this guidance include any measure that does not meet the specific requirements contained in each of the measures in E.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes incident reporting comparable to the requirements within E.1 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage).

E.2 Remote Access (RBPS 8):

E.2.1 Facilities with remote access to critical cyber systems must define allowable remote access and rules of behavior for issues related to remote access (e.g., Internet, Virtual private network (VPN), gateways, routers, firewalls, wireless access points, modems, vendor maintenance connections, Internet Protocol (IP), address ranges). Rules of behavior must be provided to and abided by all employees and contractors with access to the critical cyber systems. The rules must describe user responsibilities and expected behavior with regard to information system

usage (e.g., appropriate Web sites, conduct of personal business), including remote access activities. Further, user activities for all remote access must be captured through systems logs.

Facilities that do not have remote access must state in the SSP that there is no remote access.

With regard to E.2, material deviations from this guidance include any measure that does not meet the specific requirements contained in each of the measures in E.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the access control comparable to the requirements within E.2 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (prevent unauthorized remote access to critical cyber systems).

E.3 Control Systems (RBPS 8):

Facilities that have control systems that directly monitor and/or control manufacturing or other physical processes that contain COI must implement the following additional cyber security measures:

E.3.1 The facility must conduct audits that measure compliance with the cyber security policies, plans, and procedures and results must be reported to senior management. Audits must be clearly documented and must occur on a regular and recurring basis and no less than every two years. Audits should identify new requirements for cyber security as well as unnecessary cyber assets.

With regard to E.3.1, material deviations from this guidance include not conducting audits that meet the requirements in E.3.1. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation meets the security comparable to the requirements within E.3.1 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage).

E.3.2 The facility must document the business need and network/system architecture for all critical cyber assets (systems, applications, services, and external connections). No new connections can be established without management authorization and documentation.

With regard to E.3.2, material deviations from this guidance include measures inconsistent with the requirements in E.3.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements within E.3.2 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage). For example, such deviations include not

documenting the business need for all critical cyber assets, not documenting the network/system architecture for all critical cyber assets, and establishing connections without management authorization and/or documentation.

E.3.3 Upon identification, the facility must disable all unnecessary system elements and must identify and evaluate potential vulnerabilities and implement appropriate compensatory security controls.

With regard to E.3.3, material deviations from this guidance include measures inconsistent with the requirements in E.3.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements within E.3.3 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage and prevent unauthorized on-site or remote access to critical cyber systems).

E.3.4 The facility must integrate cyber security into the system lifecycle for all critical cyber assets from system design through procurement, implementation, operation, and disposal.

With regard to E.3.4, material deviations from this guidance would include measures inconsistent with the requirements in E.3.4. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements of E.3.4 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage).

E.3.5 The facility must ensure that service providers and other third parties with responsibilities for and access to critical cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel surety requirements for facility employees (reference Section F.3).

With regard to E.3.5, material deviations from this guidance would include personnel security measures inconsistent with requirements in E.3.5. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements of E.3.5 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage).

E.3.6 The facility must identify and document systems boundaries and implement security controls to limit access across those boundaries.

With regard to E.3.6, material deviations from this guidance would include measures inconsistent with the requirements in E.3.6. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation meets the security comparable to the requirements within E.3.6 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage and prevent unauthorized on-site or remote access to critical cyber systems).

E.3.7 The facility must monitor the critical networks in real-time for unauthorized or malicious access and alerts, recognizes and logs events and incidents.

An intrusion detection system (IDS) must be used to monitor networks. An IDS is a system 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 (i.e., captures and analyzes all network traffic) or host-based (i.e., installed on, and analyzing traffic for, a single device).

With regard to E.3.7, material deviations from this guidance include monitoring critical networks via a system which is inconsistent with the requirements in E.3.7. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements within E.3.7 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage and prevent unauthorized on-site or remote access to critical cyber systems).

E.3.8 The facility must have a defined incident response system for cyber incidents. This must include either an individual or computer emergency response function that can be contacted in the event of a cyber emergency and is trained to identify, contain, and resolve a cyber intrusion, denial-of-service attack, virus, worm attack, or other cyber incident.

With regard to E.3.8, material deviations from this guidance would include measures inconsistent with the requirements in E.3.8. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements of E.3.8 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage).

E.3.9 The facility must have back-up power for all critical cyber systems should an emergency or incident occur.

With regard to E.3.9, material deviations from this guidance include any measure that does not meet the specific requirements contained in E.3.9. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the security comparable to the requirements of E.3.9 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage and prevent unauthorized on-site or remote access to critical cyber systems). For example, material deviations from this guidance include implementing a compensatory measure rather than back-up power during emergencies or system failures.

E.3.10 The facility must have continuity of operations plans, IT contingency plans, and/or disaster recovery plans.

With regard to E.3.10, material deviations from this guidance would include implementing measures inconsistent with the requirements in E.3.10. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements of E.3.10 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 8 (deter cyber sabotage).

Facilities that do not have control systems must state in the SSP that there are no control systems.

Section F: Security Management Measures

(RBPS 7, 10 – 12 and 15 - 18)

Background on Security Management

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.

F.1 Maintenance, Inspection and Testing of Security Equipment (RBPS 10):

It is necessary to maintain reliability of security systems. This includes conducting regular tests, making repairs as required, and installing improvements to the security systems as necessary. Complying with the manufacturers' instructions and specifications for frequency of testing, repair, and replacement schedules increases the likelihood that the physical security equipment will function as it is expected. Facilities must include all of the following in their SSP for all appropriate security equipment:

F.1.1 The facility must have 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.

F.1.2 The facility must have identified individual(s) responsible for inspection, testing, and maintenance of security systems. These individuals must be trained and capable of performing all responsibilities.

F.1.3 The facility must maintain all security systems in working order and according to manufacturer's specifications through daily use, inspections, testing, or a preventative maintenance program.

F.1.4 The facility must implement temporary/compensatory measures in the event of security system failures or outages to include deploying back-up hardware and adding security or operations personnel patrols to affected areas. See additional information on back-up power and compensatory measures within Section B.

With regard to F.1, material deviations from this guidance would include implementing inspections, testing, and maintenance of security systems inconsistent with the requirements contained in each of the measures in F.1, to include implementing measures without documentation such as procedures and policies. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the inspection, testing, and maintenance comparable to the requirements within F.1 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 10 (ensure security systems and equipment are in good working order and are inspected, tested, calibrated, and otherwise maintained).

F.2 Training (RBPS 11):

By performing proper security training, exercises, and drills, a facility enables its personnel to be better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders.

F.2.1 Facilities must develop and implement a recurring (at a minimum of biennially) Security Awareness and Training Program (SATP) for all facility personnel and for contractors with security responsibilities.

F.2.1.1 Training topics must include:

- Emergency procedures,
- Crisis management plans,
- Suspicious persons and vehicles, and
- Recognition and reporting of security incidents.

F.2.1.2 This training must highlight the COI and associated security concern and focus on identifying suspicious activities or security incidents with regard to the security concern.

F.2.1.3 Facilities tiered for **Theft/Diversion** COI must include within their training identifying suspicious persons attempting to gain access to the perimeter or critical asset(s), suspicious persons attempting to remove COI, methods of concealing COI, suspicious COI orders, etc.

F.2.1.4 Facilities tiered for **Release** COI must include within their training identifying suspicious vehicles, vehicle screening and inspections, and recognizing explosive devices.

F.2.2 The SATP must include recurring (at a minimum of biennially) training for senior officials (e.g. Corporate Security Officer, Site Security Officer, Alternative Site Security Officer, and Cyber Security Officer) on topics which include:

- Security laws and regulations,
- Threats,
- Security organization, and
- Security duties and responsibilities.

F.2.3 For facilities that employ security personnel, the SATP must include recurring (at a minimum of biennially) training on topics which include:

- Emergency procedures,
- Crisis management planning,
- Operation of security equipment, and
- Testing and maintenance of security equipment and methods of screening persons and vehicles, where applicable.

With regard to F.2, material deviations from this guidance include measures that do not include a training program that meets the specific measures contained in each of the measures in F.2. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the training comparable to the requirements of F.2 and how the measure accomplishes sufficient security required within relevant portions of RBPS 11 (ensure proper security training of facility personnel). For example, such deviations include providing training to select but not all facility employees, providing training inconsistent with the topics identified above, and providing training on a frequency less than biennially.

F.3 Personnel Surety (RBPS 12):

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. See C.3 for further requirements related to access control and credentials.

F.3.1 Facilities must identify and maintain lists of all affected individuals. Affected individuals are defined as:

- facility personnel 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.

F.3.2 Facilities must verify and validate the identity of all affected individuals by a government issued ID or identification document as listed on the I-9 form prior to granting access to restricted area(s) and critical asset(s). Verifying ID includes comparing the picture on the card with the owner, comparing the physical characteristics against the person's physical appearance, checking for tampering, reviewing both sides of the card, and checking the expiration date. If identity cannot be verified, the individual cannot be granted access to the critical asset(s).

F.3.3 Facilities must verify and validate the legal authorization to work of all affected individuals by utilizing the I-9 process prior to granting access to restricted area(s) and critical asset(s). For employees who were hired prior to the Immigration Reform and Control Act of 1986 (Public Law 99-603), facilities must verify and maintain evidence of proof of continuous employment since November 7, 1986. If legal authorization to work cannot be verified, the individual cannot be granted access to the restricted areas or critical asset(s).

F.3.4 Facilities must conduct a criminal history check on all affected individuals through a third party background investigation company, national program, or local law enforcement agency. This background check must check national, state, and local resources for a timeframe of no fewer than five years and the report must identify all felonies, at a minimum.

F.3.5 Facilities must have a process for adjudicating the results of these background checks and determining access restrictions in a reasonable manner.

F.3.6 Upon notification from DHS, facilities must implement a process to identify all affected individuals with terrorist ties. Facilities must comply with the requirements described in the CFATS Personnel Surety Program implementation notice and must implement one or more of the options allowed under the CFATS Personnel Surety Program for identifying individuals with terrorist ties.[11]

F.3.7 Facilities must escort all visitors that do not have all types of background investigations as described above via an approved and trained escort. Individual(s) serving as escorts must have background checks, have been trained on escort procedures, be instructed to and capable of reporting suspicious activities or violations which occur while they are escorting, provide escort either in-person or via dedicated camera observation and escort no more than five (5) individuals at one time.

F.3.8 Facilities must maintain documentation (at a minimum: employee name, how the required checks were conducted, and the results of the checks) of background checks for all current affected individuals in order to demonstrate compliance with personnel surety requirements[12].

With regard to F.3, material deviations from this guidance include a lack of personnel surety measures or any program that does not meet the specific measures contained in each of the measures in F.3. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the personnel surety measures comparable to the requirements of F.3 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 12 (verify and validate of identity, legal authorization to work, criminal history, and terrorist ties for all affected individuals). For example, such deviations include utilizing a different document or method to verify identity, legal authorization to work and criminal history; conducting criminal background checks which do not include national,

[11] The Department is not yet applying RBPS 12(iv) to Tiers 3 and 4 – see footnote 1 on page 6 of this document for a more detailed discussion of the Department's plans for implementation of RBPS 12(iv). DHS will notify EAP facilities when their obligation to conduct terrorist ties checks for affected individuals begins.

[12] Although not protected by the Privacy Act of 1974, facilities are required to protect information under existing laws (as applicable), which provide protections for the information that has been collected by the facility in order to comply with RBPS 12(i-iii). While under CFATS, no specific controls are required for information collected by high-risk chemical facilities with regard to RBPS 12(i-iii), DHS expects that high-risk chemical facilities will protect and safeguard the information in accordance with any other federal, state, or local privacy laws that are applicable to the collection of the information, just as they would for other similar information collected under a facility's normal business practices that is not related to the CFATS Program.

state, and local checks or do not report felonies; conducting criminal background checks dating back less than five (5) years; not providing escorts for visitors with access to restricted areas or critical assets that have not undergone background checks; and permitting visual verification of an existing federal credential that conducts identity checks, criminal history checks, or validates the legal authorization to work.

F.4 Incident Reporting and Investigations (RBPS 15 and 16):

Facilities must 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.

F.4.1 Facilities must have written procedures which define incident reporting and investigation protocols, which include the identification of the types of incidents to report, to whom to report incidents, and the responsibilities of all individuals with reporting and investigation roles.

F.4.2 Facilities must report the following 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)[13]:

- 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. Similarly, it is recommended that a facility report the incident immediately to local first responders via 911 if the incident has concluded, but

[13] Note that this measure in no way affects the obligation under the rail transportation security regulations in 49 CFR Part 1580 of a facility defined as a "rail hazardous materials shipper" or a "rail hazardous materials receiver located within an HTUA" (High Threat Urban Area, as defined in 49 CFR § 1580.3) to report significant security concerns to DHS in accordance with 49 CFR § 1580.105. Please contact surfacefrontoffice@tsa.dhs.gov for further information on this regulatory requirement.

an immediate emergency response is necessary. Once the incident has concluded and any immediate resulting emergency has been mitigated, a facility should use a nonemergency number to inform local first responders (if they had not already been contacted) and DHS. Within DHS, incidents must be reported to the NICC. In addition to the NICC, a facility may wish to contact its local FBI Field Office, whose phone number can be found online at www.fbi.gov/contact/fo/ focities.htm.

F.4.3 Facilities must have a security incident investigation program to thoroughly investigate all significant security incidents through either internal or third party personnel, who are qualified and trained to perform such investigations.

F.4.4 Facilities must document "lessons learned" from security incidents and incorporate these into employee training programs and policies.

With regard to F.4, material deviations from this guidance include any measure that does not meet the specific requirements contained in each of the measures in F.4. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation in the SSP of how the deviation accomplishes the reporting measures comparable to the requirements within F.4 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 15 (report significant security incidents) and RBPS 16 (identify, investigate, report, and maintain records of significant security incidents and suspicious activities). For example, such deviations include implementing reporting and/or investigation programs without written procedures, reporting security incidents inconsistent with the items listed herein, and not documenting lessons learned as part of reporting and ongoing training programs.

F.5 Security Organization (RBPS 17):

Facilities must identify security officials, as well as the organization within the company that is 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 how large or complex a facility or its ownership structure is. 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, as further described below.

F.5.1 Facilities must define a security organizational structure in writing that identifies specific security duties and responsibilities.

F.5.2 Facilities must designate a Site Security Officer (SSO), Alternate SSO, Cyber Security Officer, and, where applicable, a Corporate Security Officer with clear responsibilities and the qualifications and training to perform all duties. Individuals serving in these roles may serve in more than one role; however, the SSO and Alternate SSO should not be the same individual unless the facility employs only one individual. Qualifications for being an SSO (or equivalent) must 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.

F.5.3 Individuals within the security organization must be designated to perform all of the following:

- Ensure all individuals responsible for security perform their duties appropriately.
- Oversee the submission of Top Screens and Security Vulnerability Assessments, and the submission and implementation of SSPs or Alternative Security Programs to DHS.
- Host DHS inspections.
- Develop, revise, and implement security policies and procedures.
- Develop, plan, and conduct security-related training.
- Maintain records.

With regard to F.5, material deviations from this guidance would include not implementing a security organization or implementing an organization inconsistent with the descriptions and qualifications identified in each of the measures in F.5. Pursuant to 6 U.S.C. § 622(c)(4)(B)(ii), this requires an explanation within the SSP of how the deviation accomplishes the security comparable to the requirements within F.5 and how the measure accomplishes the sufficient security required within relevant portions of RBPS 17 (establish officials and an organization responsible for security and compliance).

F.6 Recordkeeping (RBPS 18):

No material deviations are permitted for this RBPS because these recordkeeping provisions are required by the regulation.

F.6.1 Per 6 CFR Part 27.255 Recordkeeping requirements, facilities must create, maintain, protect, store, and make available for inspection by DHS all of the below records and other records related to its security program in order to demonstrate compliance with their security plan.

F.6.2 The facility must retain security training records, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a). The training records include the date and location of each training session, time of day and duration of each session, a description of the training, the name and qualifications of the instructor, a legible list of attendees (including each attendee's signature), and the results of any evaluation or testing. See 6 CFR § 27.255(a)(1).

F.6.3 The facility must retain records of drills and exercises, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a). Such records include, 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 that may improve the SSP. See 6 CFR § 27.255(a)(2).

F.6.4 The facility must retain records of incidents and breaches of security, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a). Such records include the date and time of occurrence, location within the facility, a description of the incident or breach, the identity of the individual(s) to whom it was reported, and a description of the response. See 6 CFR § 27.255(a)(3).

F.6.5 The facility must retain records of maintenance, calibration, and testing of security equipment, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a). Such records include 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. See 6 CFR § 27.255(a)(4).

F.6.6 The facility must retain records of security threats, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a). Such records include the 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. See 6 CFR § 27.255(a)(5).

F.6.7 The facility must retain records of audits of the facility's SSP or Security Vulnerability Assessment, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a). Such records include, for each audit, a record of the audit, results of the audit, names(s) of the person(s) who conducted the audit, and a letter certified by the covered facility stating the date that the audit was conducted. See 6 CFR § 27.255(a)(6).

F.6.8 The facility must retain all Letters of Authorization and Approval from DHS and documentation identifying the results of audits and inspections conducted pursuant to §27.250, in paper or electronic format, for at least three (3) years. See 6 CFR § 27.255(a)(7).

F.6.9 The facility must retain records of submitted Top-Screens, Security Vulnerability Assessments, SSPs/Alternative Security Programs/Expedited Approval Submissions, and all related correspondence with the Department, in paper or electronic format, for at least six (6) years. See 6 CFR § 27.255(b).

Resources

Business Continuity Guidelines, ASIS International, www.asisonline.org

Department of the Army, "Physical Security", Army Techniques Publication (ATP) 3-39.32, April 2014

Introduction to Security, 8th Edition, Robert J. Fischer, Edward Halibozek, and Gion Green, April 2008

National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

Physical Security Manual, ASIS International, www.asisonline.org

Protection of Assets Manual, ASIS International, www.asisonline.org

Risk-Based Performance Standards Guidance Document, May 2009

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, August 2013

Title 29 – Labor, Subtitle B – Regulations Relating to Labor, Chapter XCII – Occupational Safety and Health Administration, Department of Labor, Part 1926 – Safety and Health Regulations for Construction

Unified Facilities Criteria 4-010-01, DOD Minimum Antiterrorism Standards for Buildings, October 2013

Unified Facilities Criteria 4-020-01, Security Engineering: Facilities Planning Manual, September 2008

Unified Facilities Criteria 4-020-04FA, Security Engineering: Electronic Security Systems, March 2005

Unified Facilities Criteria 4-022-01, Security Engineering: Entry Control Facilities / Access Control Points, May 2005

Attachment 1: Certification Under Penalty of Perjury

Facilities choosing to submit under the Expedited Approval Program must submit a certification, signed under penalty of perjury that meets the requirements of 6 U.S.C. § 622(c)(4)(C) along with the SSP. The following pages provide the certification for facilities to fill out and submit via CSAT either as part of or an attachment to the SSP.

CERTIFICATION FOR EXPEDITED APPROVAL

I am the owner or operator of [**Name of Facility Here**][**CFATS Facility ID Number Here]**.

I am familiar with the requirements of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (Pub. L. 113-254) and part 27 of title 6 of the Code of Federal Regulations.

I am familiar with the site security plan being submitted for [**Name of Facility Here**] and certify that:

- The site security plan includes security measures that, in combination, appropriately address the security vulnerability assessment and the risk-based performance standards for security for the facility;
- The security measures in the site security plan do not materially deviate from the guidance for expedited approval facilities except where indicated in the site security plan;
- Any deviations from the guidance for expedited approval facilities in the site security plan meet the risk-based performance standards for the tier to which the facility is assigned;
- The site security plan includes explanations of how it meets the risk-based performance standards for any material deviations from the guidance for expedited approval facilities;
- I have visited, examined, documented, and verified that the facility meets the criteria set forth in the site security plan;
- The facility has implemented all of the required performance measures outlined in the site security plan or set out planned measures that will be implemented within a reasonable time period stated in the site security plan;
- Each individual responsible for implementing the site security plan has been made aware of the requirements relevant to the individual's responsibility contained in the site security plan and has demonstrated competency to carry out those requirements;
- I have committed, or in the case of planned measures will commit, the necessary resources to fully implement the site security plan; and
- Any planned measures in the site security plan include an adequate procedure for addressing events beyond my control in implementing any planned measures.

I certify under penalty of perjury that the foregoing is true and correct.

Executed on _____
(Date)

Signature _____

_____
(Print Name and Title)

Attachment 2: Expedited Approval SSP Example

Note: The example includes a CVI coversheet, header, and footer. These are included as examples of properly marking Expedited Approval SSPs. The information contained within the example is fictitious and, therefore, not CVI.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

Requirements for Use

NONDISCLOSURE

WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 CFR 27.400. Do not disclose to persons without a "need to know" in accordance with 6 CFR § 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR § 27.400(h) and (i).

By reviewing this cover sheet and accepting the attached CVI you are agreeing to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached CVI.

Access

This information may not be further disclosed except to individuals who meet the following requirements:

- All individuals must be CVI Authorized Users
- All individuals must demonstrate a valid need-to-know for specific CVI

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container.
Do not leave this document unattended.

Transmission: You may transmit CVI by the following means to a CVI Authorized User with a need to know.

Hand Delivery: CVI may be hand carried as long as access to the material is controlled while in transit.

Email: Encryption should be used. If encryption is not available, send CVI as an encrypted attachment or password protected attachment and provide the password under separate cover. Whenever the recipient forwards or disseminates CVI via email, place that information in an attachment. **Do not send CVI to personal, non-employment related email accounts.**

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as CVI. Envelope or container must bear the complete name and address of the sender and addressee. The envelope must bear the following statement below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**."

Fax: Secure faxes are encouraged, but not required. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: Secure Telephone Unit/Equipment are encouraged, but not required. Use cellular or cordless phones to discuss CVI only in exigent circumstances. Do not engage in a conversation in a public place or in environments that will allow anyone that does not have a need to know to overhear the conversation.

Reproduction: Ensure that a copy of this sheet is the first and last page of all reproductions containing CVI. Clear copy machine malfunctions and ensure all paper paths are checked for CVI. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this CVI document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use a CVI document to create a product that is released to the public such as an advisory, alert or warning. In this case, the product must not reveal any information that:

- Exposes vulnerabilities of identifiable critical infrastructure or protected systems of a facility;
- Is proprietary, business-sensitive, or trade secret;
- Relates specifically to the submitting person or entity (explicitly or implicitly).

Derivative Products

Mark any newly created document containing CVI with "CHEMICAL-TERRORISM VULNERABILITY INFORMATION" on the top of each page that contains CVI and the distribution limitation statement at 6 CFR § 27.400(f)(3) on the bottom.

Place a copy of this cover page over all documents containing CVI.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

Facility Name: CFATS - Facility 1

CSAT Facility ID: 6000000

Expedited Approval Site Security Plan

Expedited Approval SSP Organization:

Section A: General Facility Information

Section B: Detection Measures (RBPS 1, 2, 3, 4, 5, 6, and 7)

Section C: Delay Measures (RBPS 1, 2, 3, 4, 5, 6, and 7)

Section D: Response Measures (RBPS 9, 11, 13, and 14)

Section E: Cyber Security Measures (RBPS 8)

Section F: Security Management Measures (RBPS 7, 10, 11, 12, 15, 16, 17, and 18)

Attachments

Section A: General Facility Information

Facility Information

CSAT Facility ID: 6000000

Facility Name: CFATS - Facility 1

Owner/Operator: CFATS Corporation

Facility Address: 1 CFATS Way
Washington, D.C. 20000

Facility Latitude 38.381122

Facility Longitude: -73.764648

Facility Type/Description:

Facility is involved in chemical distribution, specifically Chlorine distribution. The facility receives COI by railcar and repackages COI into smaller containers. The facility ships and sells COI.

Co-Located Facility Information: Yes☐ No☐

The facility is co-located with CFATS - Facility 2.

Facility Personnel

Site Security Officer (SSO) (Name and/or Title): Mr. Bruce Jones

Phone: (888)123-4567 x1

Alternate SSO (Name and/or Title): Ms. Karen Smith

Phone: (888)123-4567 x2

Corporate Security Officer (Name and/or Title): Ms. Mary Miller

Phone: (888) 123-4567 x3

Cyber Security Officer (Name and/or Title):	Mr. Paul Johnson
Phone:	(888)123-4567 x4
Corporate Cyber Security Officer (Name and/or Title):	Mr. Al Thomas
Phone:	(888)123-4567 x5
Number of Facility Personnel:	25
Full-Time:	15
Part-Time:	5
Full-Time Contractor:	5
Part-Time Contractor:	0
On-Site Security:	0
Work Shifts:	M-F (9am-5pm)
Operational 24/7	Yes☐ No☐

First Responder Information

Local Fire Department:	Washington Fire Department
Phone:	(123)456-7890
Local Law Enforcement:	Washington Police Department
Phone:	(123)456-7899

Chemical Information

COI	Tier	Security Issue	Portable (Y/N)	Container Type	Receive (Y/N)	Manufacture (Y/N)	Ship/Sell (Y/N)
Chlorine	3	Theft/Diversion	Y	150lb. Cylinders	N	N	Y
Chlorine	4	Release (Toxic)	N	Bulk Tank	Y	N	N

Facility Assets

Asset Name: Chlorine Bulk Storage Tank

Asset Description:

Outdoor storage area containing 1,000,000 pounds of pressurized liquefied gas of Chlorine stored in a bulk storage tank. The tank is locked in a 4-sided cage. This area is located on the outside of the northeast wall of the facility and is enclosed by the perimeter fence line. Roving patrols frequent this asset during operational hours. There is a key control policy in place limiting access to only authorized individuals. There is also a 24/7 leak detection system attached to this asset.

Asset Name: Chlorine Cylinder Storage Area

Asset Description:

Indoor asset area containing repackaged Chlorine in 150lb. cylinders. The asset is located in the southeast corner of the facility's warehouse and is patrolled frequently by facility personnel. Additionally, the building is covered by IDS, which is activated during non-operational hours. Only authorized individuals have access to the asset.

Asset Name: _____

Asset Description:

Asset Name: _____

Asset Description:

Facility Attachments

☐ The facility verifies that it has uploaded a plot plan or facility schematic as an attachment to this security plan.

Describe other attachments uploaded (e.g. descriptions of deviations to security measures):

Facility Plot Plan
Overhead Facility Picture
Picture of Bulk Storage Tank asset area
Picture of Indoor 150 lb. Cylinder asset area

Section B: Detection Measures

(RBPS 1, 2, 3, 4, 5, 6, and 7)

B.1 Detection (RBPS 1, 2, 4, 6 and 7)

The facility has a monitoring capability at the perimeter, critical asset(s), or a combination of the two which allows for the identification of the presence of an intrusion in the area(s) containing the critical asset(s), including one or more of the following:

B.1.1 ☐ Intrusion Detection System (IDS) with the following attributes:

B.1.1.1 ☐ IDS includes one or more of the following types of sensors and is deployed in accordance with the manufacturer's specifications: infrared (IR) sensors, microwave sensors, fiber-optic sensors, buried cable, magnetic switches, balanced magnetic switches, volumetric motion sensors, glass-breakage sensors, and passive IR motion sensors.

B.1.1.2 ☐ IDS is activated at all times when another detection method (see B.1.2 and B.1.3) is not available.

B.1.1.3 ☐ IDS covers either all perimeter entry point(s) (doors and windows, as applicable) or all access point(s) leading to the critical asset(s).

B.1.1.4 ☐ IDS alarms to a responsible and trained individual(s) to initiate a response either through local alarm, central station, auxiliary connection (police or fire), or proprietary station.

B.1.1.5 ☐ IDS includes backup power or personnel are deployed to provide detection during system outages or failures.

B.1.2 ☐ Closed Circuit Television (CCTV) with the following attributes:

B.1.2.1 ☐ CCTV includes the integration of cameras, recorders, switches, keyboards, and monitors.

B.1.2.2 ☐ CCTV ensures the capability to detect an object, recognize the type of object, and identify the details of the object and is deployed in accordance with manufacturer's specifications.

B.1.2.3 ☐ CCTV is activated at all times when another detection method (see B.1.1 and B.1.3) is not available.

B.1.2.4 ☐ CCTV covers all perimeter entry point(s) (doors and windows, as applicable), all critical asset(s) access point(s), or all critical asset(s) area(s).

B.1.2.5 ☐ CCTV has appropriate security lighting (see B.2.1).

B.1.2.6 ☐ CCTV is monitored by a dedicated and trained individual(s) or is equipped with motion detection to alarm to a responsible and trained individual(s) to initiate a response.

B.1.2.7 ☐ CCTV includes backup power or personnel are deployed to provide detection during system outages or failures.

B.1.2.8 ☐ CCTV includes information transmission via one of the following methods: metallic video cables, RF transmission, and/or fiber-optic cable.

B.1.3 ☐ Facility personnel and/or on-site security capable and trained to provide detection of an intrusion are either dedicated to the perimeter or critical asset(s) access point(s) or conduct roving patrols of perimeter or critical asset(s) area(s)

For Theft/Diversion Facilities only: The facility has identified their level of delay and included details related to their detection in either B.1.4 or B.1.4.1.

B.1.4 ☐ The facility has one layer of delay. Describe how the combination of the above measures ensures that the facility has a monitoring capability with breaks of no more than four (4) hours.

Theft/Diversion critical asset area is protected within the warehouse which has an IDS on all perimeter doors and windows that is activated during non-operational hours. The IDS is monitored by a third party company who alerts the police and facility management if the IDS alarms. Facility employees are regularly within the warehouse, conducting patrols and inventories during operational hours. The combination of these measures provides for continuous monitoring.

B.1.4.1 ☐ The facility has more than one layer of delay, only one of which is a fence. Describe how the combination of the above measures ensures that the facility has a monitoring capability with breaks of no more than eight (8) hours.

☐ The facility is not regulated for any Theft/Diversion COI.

For Release facilities only:

B.1.4.2 ☐ The facility has continuous monitoring through a detection method described above to ensure there are no breaks in detection capability, OR

Describe:

See below material deviation.

☐ The facility is not regulated for any Release COI.

For Sabotage facilities only:

B.1.4.3 ☐ The facility can detect a COI contamination prior to shipment through one or more of the following:

☐ Continuous monitoring through dedicated sources via one of the methods described above;

☐ 100% screening and inspections for contraband upon entering the facility or critical asset(s) area(s) (See C.3.1.3); or

☐ Shipping procedures requiring 100% inspection of shipments and tamper evident devices upon egress (see C.5.8).

Describe:

N/A

☐ The facility is not regulated for any Sabotage COI.

B.2 Security Lighting (RBPS 1, 2, and 4):

B.2.1 ☐ The facility provides and maintains sufficient illumination levels (at a minimum of 5 foot-candles for indoor storage areas and 10 foot-candles for outdoor storage areas) to permit individual(s) to perform their duties, provide appropriate surveillance, and properly utilize all security equipment (e.g. CCTV systems).

B.3 Inventory Control (RBPS 5 and 6):

B.3.1 ☐ The facility has written procedures for inventory control, which identify at least one person as responsible for conducting inventories and outline the roles and responsibilities of individuals charged with conducting inventories. The facility maintains records, either in the form of logs, charts, or electronic systems, which demonstrate that the inventories have been conducted and when and by whom.

B.3.2 ___ The facility either:

☐ Has process control systems that monitor the level, weight, volume, or

☐ Conducts COI inventory physically through documented inventory checks (e.g. cycle counts) at a minimum of weekly.

Detection Planned Measures

☐ The facility does not have existing security measures for one or more of the required items above, but will implement the security measure through a planned measure no later than twelve (12) months of approval as described below:

Material Deviation

☐ The facility has materially deviated from the above detection measures; however, the facility has incorporated compensatory measures, which offer comparative security to the requirements in Section B - Detection and meet the security concerns in the relevant portions of the RBPS as follows:

This is a material deviation for Section B.1.4.2. The Release COI is not covered by IDS or CCTV and personnel are only monitoring during operational hours. The COI is located within a restricted cage within the perimeter fence line. There is a key control policy in place limiting access to only authorized individuals and any tampering with the asset locking system would be evident.

The facility achieves detection of the outdoor storage area by utilizing roving patrols during operational hours. During non-operational hours, the facility relies on a leak detection system which is in place all hours and will alert facility management of any leaks. The leak detection system also has an automatic shutoff capability and the tank is completely surrounded by a containment dike which has the capability to hold all contents without any risk of further release. This detection coupled with this mitigation allows the facility to achieve a comparable level of detection to the requirements within B.1.4.2 and the asset monitoring requirements in RBPS 1, 2, and 4.

Section C: Delay Measures (RBPS 1, 2, 3, 4, 5, 6, and 7)

C.1 Human Barriers (RBPS 1, 2, 4, 6 and 7):

C.1.1 ☐ The facility utilizes barriers which completely enclose the perimeter or critical asset(s) utilizing walls or security fences.

C.1.1.1 ☐ Fences are constructed of chain link, barbed wire, or concertina and are a minimum of seven (7) feet high (including topper, where applicable).

C.1.1.2 ☐ Walls are constructed of brick, cinder block, poured concrete, wood, or metal panel are a minimum of seven (7) feet high (including topper, where applicable).

C.1.1.3 ☐ The facility has at least two layers of barriers enclosing the facility or all critical asset(s), one of which is made of walls constructed of brick, cinder block, poured concrete, wood, or metal panel in order to justify a less frequent level of detection in B.1.4.1.

C.1.2 ☐ The facility utilizes locking mechanisms for entry points to the perimeter or critical asset(s) which include one or more types: locksets, deadbolts, magnetic locks, padlocks, cam locks, mortise locks, and/or cylinder locks. Access points are locked at all times when access point is not in use or manned.

C.1.3 ☐ The facility maintains a key/lock, combination, and/or access credential control and accountability program which ensures keys, locks, combinations and access credentials are only issued to authorized individuals, are collected upon termination of employment or change in work status, are periodically inventoried, and are changed when there is a loss or suspicion of compromise or upon termination of employment. A periodic inventory of keys, combinations and/or access controls is conducted at a minimum of annually.

C.2 Vehicle Barriers for Release COI (RBPS 1, 2, and 4):

C.2.1 ☐ The facility employs vehicle barriers such as bollards, berms, ditches, revetments, cables, moats, and/or jersey barriers at the perimeter or critical asset(s) in order to reduce the likelihood of accessing the facility or critical asset(s) by force or employing a Vehicle-Borne Improvised Explosive Device (VBIED) in close proximity to the release COI.

C.2.2 ☐ The facility establishes a standoff distance for Release COI assets.

☐ The facility is not regulated for Release COI.

C.3 Access Control (RBPS 3 and 7):

C.3.1 ☐ The facility established a personnel identification program which includes validating the identity of all visitors requesting access to the facility or critical asset(s) via government-issued photo identification (ID) card.

The facility further accomplishes personnel identification through one or more of the following:

C.3.1.1 ☐ The facility permits access to the facility or restricted area(s) to only those on approved entry lists and conducts checks of government-issued photo ID cards to verify that entering employees, contractors or visitors are on the lists.

C.3.1.2 ☐ The facility provides company-issued, facility-specific photo IDs, or access credentials to individuals permitted access to the facility or restricted areas of the facility.

C.3.1.3 ☐ The facility utilizes employee training to recognize and identify facility personnel granted access.

C.3.2 ☐ The facility restricts access within the perimeter or restricted area(s) to only authorized individuals by one or more of the following means:

C.3.2.1 ☐ An electronic access control system (ACS)

C.3.2.2 ☐ Physical locking mechanisms

C.3.2.3 ☐ Implementation by facility personnel (e.g. security guards or supervisors) of screening and inspection procedures

Describe:

The facility has an ACS on all entry doors to the warehouse (some exit only doors do not have ACS but do not have hardware allowing entry) where the Theft/Diversion COI are stored and utilizes physical locking mechanisms on the main vehicle gate and restricted outdoor storage cage.

For Release and Sabotage facilities only:

C.3.3 ☐ The facility conducts an inspection of items brought into the facility or restricted area(s).

☐ The facility is not regulated for any Release or Sabotage COI.

For Release facilities only:

C.3.4 ☐ The facility conducts screening and inspections of vehicles prior to allowing access to the perimeter and/or Release critical asset(s).

☐ The facility is not regulated for any Release COI.

C. 4 Receiving Procedures (RBPS 5 and 6):

C.4.1 ☐ The facility plans in advance all in-bound shipments of COI.

C.4.2 ☐ The facility ensures COI is being received from a known, pre-approved shipper.

C.4.3 ☐ The facility inspects trucks, trailers and rail cars, where applicable, upon entering the facility or restricted area(s).

C.4.4 ☐ The facility transfers COI from unloading areas to storage or process areas in an expeditious manner in order to ensure the COI is not left unattended in the unloading area.

☐ The facility does not receive COI.

C.5 Shipping / Selling Procedures Shipping Procedures (RBPS 5, 6, and 7):

C.5.1 ☐ The facility plans and approves all shipments of COI in advance using known, pre-approved, carriers.

C.5.2 ☐ The facility has procedures or practices to ensure multiple levels of review and validation of all shipments.

C.5.3 ☐ The facility has a Know Your Customer program or similar practice which ensures customers of COI are properly vetted to include verifying a customer's identity, business location, financial status, and COI end use.

C.5.4 ☐ The facility has a procedure or practice to refuse the sale of COI unless customers meet customer vetting and identification procedures.

C.5.5 ☐ The facility establishes normal business-to-business payment terms and methods that prevent cash sales to customers.

C.5.6 ☐ The facility documents all sales and shipments of COI including, the method of shipment, carrier information, the times and dates of shipments, and the destination. The records are maintained a minimum of three years.

C.5.7 ☐ The facility utilizes tamper-evident mechanisms to identify tampering with COI prior to and during shipment.

C.5.8 ☐ The facility inspects trucks, trailers, and rail cars, where applicable, prior to loading and departing.

C.5.9 ☐ The facility confirms all shipments have arrived to their final destination.

C.5.10 ☐ The facility ensures systems are in place to track and protect shipments en route to their destinations, such as driver call-in schedules, GPS tracking, etc.

Delay Planned Measures

☐ The facility does not have existing security measures for one or more of the required items above, but will implement the security measure through a planned measure no later than twelve (12) months of approval as described below:

Material Deviation

☐ The facility has materially deviated from the above delay measures; however, the facility has incorporated compensatory measures, which offer comparative security to the requirements in Section C - Delay and meet the security concerns in the relevant portions of the RBPS as follows:

Section D: Response Measures (RBPS 9, 11, 13, and 14)

D.1 Response Planning

D.1.1 ☐ The facility has a defined emergency and security response organization in order to respond to site emergencies and security incidents.

D.1.2 ☐ The facility has a crisis management plan which includes emergency response procedures, security response plans, and post-incident security plans (post-terrorist attack, security incident, natural disaster, etc.).

For Release facilities only:

D.1.2.1 ☐ The facility has additional portions to their crisis management plan, which include emergency shutdown plans, evacuation plans, re-entry/recovery plans, and community notification plans to account for response to Release COI.

☐ The facility is not regulated for Release COI.

D.1.3 ☐ The facility has designated individual(s) responsible for executing each portion of the crisis management plan and individual(s) have been trained to execute all duties.

D.1.4 ☐ The facility has the appropriate resources (staff, emergency/response equipment, building space, communications equipment, process controls/safeguards, etc.) to execute all response plans. Emergency equipment includes at least one of the following:

- A radio system that is redundant and interoperable with law enforcement and emergency response agencies.
- At least one backup communications system, such as cell phones/desk phones.
- An emergency notification system (e.g., a siren or other facility-wide alarm system).
- Automated control systems or other process safeguards for all process units to rapidly place critical asset(s) in a safe and stable condition and procedures for their use in an emergency.
- Emergency safe-shutdown procedures for all process units.

D.1.5 ☐ All facility personnel have been trained on all response plans and response plans are exercised on a regular basis and at a minimum of biennially.

D.1.6 ☐ The facility has an active outreach program with local first responders (Police Department and Fire Department) which includes providing response documentation to agencies, providing facility layout information to agencies, inviting agencies to facility

orientation tours, notifying agencies of the facility's COI (regulated COI and other chemical holdings identified on Appendix A) and security concern, and maintaining regular communication with agencies.

D.2 Elevated and Specific Threats (RBPS 13 and 14):

D.2.1 ☐ The facility has a documented process for increasing security measures commensurate to the designated threat level during periods of elevated threats tied to the National Terrorism Advisory System (NTAS) and when notified by DHS of a specific threat.

D.2.2 ☐ The facility will begin to execute security measures for elevated and specific threats within 8 hours of notification.

D.2.3 ☐ The facility will execute the following measures as a result of an elevated or specific threat:

- Coordinate with Federal, state, and local law enforcement agencies.
- Increase detection efforts through either dedicated monitoring of security systems (IDS or CCTV), increased patrols of the perimeter and/or asset area(s), or stationing of personnel at access points and/or asset area(s).
- For *Theft/Diversion and Sabotage* facilities only, increase frequency of outbound screening and inspections.
- For *Sabotage* facilities only, increase monitoring of outbound shipments.
- For *Release* facilities only, increase frequency of inbound screening and inspections.

Response Planned Measures

☐ The facility does not have existing security measures for one or more of the required items above, but will implement the security measure through a planned measure no later than twelve (12) months of approval as described below:

This is a planned measure for Section D.1.2 and D.1.2.1

The facility will implement a Crisis Management Plan (CMP) within six months of approval. The CMP will list the roles, responsibilities, and assignments of emergency response personnel. The CMP will also include contingency plans, evacuation plans, security response plans, emergency response plans, emergency shutdown plans, re-entry/recovery plans, post-incident security plans, and community notification plans. Additionally, the facility will share the plan with local response agencies and hospitals. The facility will add this CMP to their training program. The facility will conduct drills and exercises with local law enforcement annually on this plan. The facility will conduct evacuation and response drills and exercises annually.

Material Deviation

☐ The facility has materially deviated from the above response measures; however, the facility has incorporated compensatory measures, which offer comparative security to the requirements in Section D - Response and meet the security concerns in the relevant portions of the RBPS as follows:

Section E: Cyber Security Measures (RBPS 8)

E.1.1 ☐ List all critical cyber assets 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. Provide the name and a brief description of each:

Process control system for Release COI Bulk Storage Tank - This system is used to monitor and control all process units. The process control system is located on site and is monitored 24x7x365 by a third party company. The system is segregated from all other cyber systems.

Cyber business system for Theft/Diversion COI - This system is an Enterprise Resource Planning (ERP) system and used in the sales and Ordering Process. The system is not located on site but in our Corporate Headquarters in Chicago, IL. The system does not have remote access capability.

E.1 Cyber Security – General (RBPS 8):

E.1.2 ☐ The facility has developed and maintains documented and distributed cyber security policies and procedures including change management policies, as applicable, to their critical cyber assets.

E.1.3 ☐ The facility has designated a trained and qualified individual(s) to manage cyber security for the facility.

E.1.4 ☐ The facility maintains account access control to critical cyber systems utilizing the least privilege concept and limits access to systems based on administrator and user roles and responsibilities.

E.1.5 ☐ The facility maintains access control lists, and ensures that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated in a timely manner when personnel leaving under adverse action and when users no longer require access.

E.1.6 ☐ The facility implements password management protocols to ensure all default passwords have been changed (where possible), enforces password structures, and implements physical controls for cyber systems where changing default passwords is not technically feasible.

E.1.7 ☐ The facility controls physical access to critical cyber assets and media.

E.1.8 ☐ The facility provides cyber security training to all employees that work with critical cyber assets.

E.1.9 ☐ The facility will report significant cyber incidents to senior management and DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

E.2 Remote Access (RBPS 8):

E.2.1 ☐ The facility defines allowable remote access and rules of behavior (e.g. Internet, Virtual private network (VPN), gateways, routers, firewalls, wireless access points, modems, vendor maintenance connections, Internet Protocol (IP), address ranges).

☐ The facility does not have remote access to critical cyber system(s).

E.3 Control Systems (RBPS 8):

E.3.1 ☐ The facility conducts audits that measure compliance with the cyber security policies, plans, and procedures and results are reported to senior management.

E.3.2 ☐ The facility documents the business need and network/system architecture for all cyber assets (systems, applications, services, and external connections).

E.3.3 ☐ The facility disables all unnecessary system elements.

E.3.4 ☐ The facility integrates cyber security into the system lifecycle for all critical cyber assets.

E.3.5 ☐ The facility ensures that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel surety requirements for facility employees.

E.3.6 ☐ The facility identifies and documents systems boundaries and implements security controls to limit access across those boundaries.

E.3.7 ☐ The facility monitors the critical networks in real-time for unauthorized or malicious access and alerts, recognizes and logs events and incidents.

E.3.8 ☐ The facility has a defined incident response system for cyber incidents.

E.3.9 ☐ The facility has backup power for all critical cyber systems.

E.3.10 ☐ The facility has continuity of operations plans, IT contingency plans, and/or disaster recovery plans.

☐ The facility does not have control systems which impact the security of the COI.

Cyber Security Planned Measures

☐ The facility does not have existing security measures for one or more of the required items above, but will implement the security measure through a planned measure no later than twelve (12) months of approval as described below:

Material Deviation

☐ The facility has materially deviated from the above cyber security measures; however, the facility has incorporated compensatory measures, which offer comparative security to the requirements in Section E – Cyber Security and meet the security concerns in the relevant portions of the RBPS as follows:

Section F: Security Management Measures

(RBPS 7, 10 – 12 and 15 - 18)

F.1 Maintenance, Inspection and Testing of Security Equipment (RBPS 10):

F.1.1 ☐ The facility has written procedures to ensure all security equipment applicable to the facility (i.e. IDS, CCTV, ACS, lighting, locking mechanisms, process controls/safeguards, etc.) is maintained in proper working order.

F.1.2 ☐ The facility has identified individual(s), who are trained and responsible for inspection, testing, and maintenance of security systems.

F.1.3 ☐ The facility maintains all security systems in working order and according to manufacturer's specifications through regular use, inspections, testing, or a preventative maintenance program.

F.1.4 ☐ The facility implements temporary/compensatory measures in the event of security system failures or outages to include deploying backup hardware and adding security or operations personnel patrols to affected areas.

F.2 Training (RBPS 11):

F.2.1 ☐ The facility developed and implements a recurring (at a minimum of biennially) security awareness and training program (SATP) for all facility personnel and contractors with security responsibilities.

F.2.1.1 ☐ Training topics include emergency procedures, crisis management plans, suspicious persons and vehicles, and recognition and reporting of security incidents.

F.2.1.2 ☐ The training highlights the COI and associated security concern and focus on identifying suspicious activities or security incidents with regard to the security concern.

For Theft/Diversion facilities only:

F.2.1.3 ☐ Theft/Diversion training includes suspicious persons attempting to gain access to the perimeter or critical asset(s), suspicious persons attempting to remove COI, methods of concealing COI, suspicious COI orders, etc.

☐ The facility is not regulated for Theft/Diversion COI.

For Release facilities only:

F.2.1.4 ☐ Release training includes identifying suspicious vehicles, vehicle screening and inspections, and recognizing explosive devices.

☐ The facility is not regulated for Release COI.

F.2.2 ☐ The SATP includes training for senior officials such as the Site Security Officer and Corporate Security Officer on topics which include security laws and regulations, threats, security organization, and security duties and responsibilities.

F.2.3 ☐ For facilities which employ security personnel, the SATP includes training on topics which include emergency procedures, crisis management planning, operation of security equipment, and where applicable, testing and maintenance of security equipment and methods of screening persons and vehicles.

F.3 Personnel Surety (RBPS 12):

F.3.1 ☐ The facility has identified all affected individuals as:

- facility personnel 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.

F.3.2 ☐ The facility verifies and validates the identity of all affected individuals by a government issued ID or identification document as listed on the I-9 form prior to granting access to restricted area(s) and critical asset(s).

F.3.3 ☐ The facility verifies and validates the legal authorization to work of all affected individuals by utilizing the I-9 process or E-Verify prior to granting access to restricted area(s) and critical asset(s).

F.3.4 ☐ The facility conducts a criminal history check on all affected individuals through a third party background investigation company, national program, or local law enforcement agency. This background check includes national, state, and local resources for a timeframe of no fewer than five years and the report identifies all felonies, at a minimum

F.3.5 ☐ The facility has a process for adjudicating the results of background checks and determining access restrictions in a reasonable manner.

F.3.6 ☐ Upon notification from DHS, the facility will implement a process to identify all affected individuals with terrorist ties. The facility will comply with the requirements

described in the CFATS Personnel Surety Program implementation notice and will implement one or more of the options allowed under the CFATS Personnel Surety Program for identifying individuals with terrorist ties.

F.3.7 ☐ The facility escorts all visitors which do not have background investigations via an approved and trained escort.

F.3.8 ☐ The facility maintains documentation (at a minimum: employee name, how the required checks were conducted, and the results of the checks) of background checks for all current affected individuals in order to demonstrate compliance with personnel surety requirements.

F.4 Incident Reporting and Investigations (RBPS 15 and 16):

F.4.1 ☐ The facility has written procedures which define incident reporting and investigation protocols, which include the identification of the types of incidents to report, to whom to report incidents, and the responsibilities of all individuals with reporting and investigation roles.

F.4.2 ☐ The facility will report all unauthorized, successful or unsuccessful breaches of the perimeter; unauthorized, successful or unsuccessful breaches of the critical asset; 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 assets 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).

F.4.3 ☐ The facility has a security incident investigation program to thoroughly investigate all significant security incidents through either internal or third party personnel, which are qualified and trained to perform all duties.

F.4.4 ☐ The facility documents “lessons learned” from security incidents and incorporates these into employee training programs.

F.5 Security Organization (RBPS 17):

F.5.1 ☐ The facility has defined a security organizational structure in writing that identifies specific security duties and responsibilities.

F.5.2 ☐ The facility has designated a Site Security Officer (SSO), Alternate SSO, Cyber Security Officer, and, where applicable, a Corporate Security Officer with clear responsibilities and the qualifications and training to perform all duties. Qualifications for being an SSO (or equivalent) 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.

F.5.3 ☐ Individuals within the security organization have been designated to perform all of the following:

- Ensure all individuals responsible for security perform their duties appropriately.
- Oversee the submission of Top Screens, Security Vulnerability Assessments, and Site Security Plans or Alternative Security Programs to DHS.
- Host DHS inspections.
- Develop, revise, and implement security policies and procedures.
- Develop, plan, and conduct security-related training.
- Maintain records.

F.6 Recordkeeping (RBPS 18):

F.6.1 ☐ The facility creates, maintains, protects, stores, and makes available for inspection by DHS certain records related to its security program.

F.6.2 ☐ The facility retains security training records, in paper or electronic format, for at least 3 years. The training records include the date and location of each training session, time of day and duration of each session, a description of the training, the name and qualifications of the instructor, a list of attendees (including each attendee's signature), and the results of any evaluation or testing.

F.6.3 ☐ The facility retains records of drills and exercises, in paper or electronic format, for at least three (3) years. Such records include, 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 that may improve the Site Security Plan.

F.6.4 ☐ The facility retains records of incidents and breaches of security, in paper or electronic format, for at least three (3) years. Such records include the date and time of occurrence, location within the facility, a description of the incident or breach, the identity of the individual(s) to whom it was reported, and a description of the response.

F.6.5 ☐ The facility retains records of maintenance, calibration, and testing of security equipment, in paper or electronic format, for at least three (3) years. Such records include 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.

F.6.6 ☐ The facility retains records of security threats, in paper or electronic format, for at least three (3) years. Such records include the 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.

F.6.7 ☐ The facility retains records of audits, in paper or electronic format, for at least three (3) years. Such records include, for each audit, a record of the audit, results of the audit, names(s) of the person(s) who conducted the audit, and a letter certified by the covered facility stating the date that the audit was conducted.

F.6.8 ☐ The facility retains all Letters of Authorization and Approval from DHS and documentation identifying the results of audits and inspections conducted pursuant to §27.250, in paper or electronic format, for at least three (3) years.

F.6.9 ☐ The facility retains records of submitted Top-Screens, Security Vulnerability Assessments, Site Security Plans/Alternative Security Programs/Expedited Approval Submissions, and all related correspondence with the Department, in paper or electronic format, for at least six (6) years.

Security Management Planned Measures

☐ The facility does not have existing security measures for one or more of the required items above, but will implement the security measure through a planned measure no later than twelve (12) months of approval as described below:

Currently all new hires undergo the criminal background checks. The facility will implement criminal background checks for all legacy employees with access to the critical assets and restricted areas within twelve months of SSP approval. Legacy employees will undergo criminal background checks at the federal, state, and county level and checks will be administered by a third party contractor, BI Checks. The facility will review all information and

adjudicate the results on case by case basis, taking into account the type of crime, time since the crime, number of crimes, and the individual's position. The facility will ensure all employees with access to the assets will have undergone background checks.

This planned measure satisfies the requirements of F.3.4.

Material Deviation

☐ The facility has materially deviated from the above security management measures; however, the facility has incorporated compensatory measures, which offer comparative security to the requirements in Section F – Security Management and meet the security concerns in the relevant portions of the RBPS as follows:

Attachments

Facility Plot Plan

Facility Overhead Picture

Asset Area 1 Picture

Asset Area 2 Picture

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

Requirements for Use

NONDISCLOSURE

WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 CFR 27.400. Do not disclose to persons without a "need to know" in accordance with 6 CFR § 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR § 27.400(h) and (i).

By reviewing this cover sheet and accepting the attached CVI you are agreeing to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached CVI.

Access

This information may not be further disclosed except to individuals who meet the following requirements:

- All individuals must be CVI Authorized Users
- All individuals must demonstrate a valid need-to-know for specific CVI

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container.
Do not leave this document unattended.

Transmission: You may transmit CVI by the following means to a CVI Authorized User with a need to know.

Hand Delivery: CVI may be hand carried as long as access to the material is controlled while in transit.

Email: Encryption should be used. If encryption is not available, send CVI as an encrypted attachment or password protected attachment and provide the password under separate cover. Whenever the recipient forwards or disseminates CVI via email, place that information in an attachment. **Do not send CVI to personal, non-employment related email accounts.**

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as CVI. Envelope or container must bear the complete name and address of the sender and addressee. The envelope must bear the following statement below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**."

Fax: Secure faxes are encouraged, but not required. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: Secure Telephone Unit/Equipment are encouraged, but not required. Use cellular or cordless phones to discuss CVI only in exigent circumstances. Do not engage in a conversation in a public place or in environments that will allow anyone that does not have a need to know to overhear the conversation.

Reproduction: Ensure that a copy of this sheet is the first and last page of all reproductions containing CVI. Clear copy machine malfunctions and ensure all paper paths are checked for CVI. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this CVI document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use a CVI document to create a product that is released to the public such as an advisory, alert or warning. In this case, the product must not reveal any information that:

- Exposes vulnerabilities of identifiable critical infrastructure or protected systems of a facility;
- Is proprietary, business-sensitive, or trade secret;
- Relates specifically to the submitting person or entity (explicitly or implicitly).

Derivative Products

Mark any newly created document containing CVI with "CHEMICAL-TERRORISM VULNERABILITY INFORMATION" on the top of each page that contains CVI and the distribution limitation statement at 6 CFR § 27.400(f)(3) on the bottom.

Place a copy of this cover page over all documents containing CVI.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION