# Subject: Sample Options for Risk-Based Performance Standards (RBPS) 12(iv) – Screening for Terrorist Ties

*Please refer to the Chemical Facility Anti-Terrorism Standards (CFATS) RBPS 12(iv) Fact Sheet
for an overall summary of how to implement the CFATS Personnel Surety Program (PSP) at your facility and comply with RBPS 12(iv).*

The Department of Homeland Security (DHS) has identified best practices amongst industry in developing and implementing the PSP. These best practices were used to create sample supplements for facilities preparing to implement the PSP.

The questions included in this sample are presented in the Chemical Security Assessment Tool (CSAT)
Site Security Plan (SSP), and may be used to develop a section on the PSP in an Alternative Security Program (ASP) or Expedited Approval Program (EAP) as well.

These sample supplements developed by DHS are voluntary tools to help facilities prepare to submit SSPs or ASPs in order to comply with RBPS 12(iv) and include the information necessary for DHS to determine if measures are sufficient, and if used, can be tailored to your specific facility and needs.

All information contained within these samples are fictional, and therefore are not appropriate to safeguard as Chemical-terrorism Vulnerability Information (CVI). This document does not contain CVI.

\*NOTE: This document is a sample and contains fictitious information. There is no actual CVI information in this document. To use this sample as a template for your own records, remove this text and the text box in the footer. When you insert actual CVI information, you must mark and protect it accordingly.

## Table of Contents

[**Sample Option 1**](#_RBPS_12(iv)_SAMPLE:)

[**Sample Option 1 and Option 2**](#_RBPS_12(iv)_SAMPLE:_1)

[**Sample Option 3 and Option 4**](#_RBPS_12(iv)_SAMPLE:_2)

## RBPS 12(iv) SAMPLE: Option 1

The facility has the following types of affected individuals:

* [x]  Facility personnel (e.g., employees, contractors) with access to the restricted areas or critical assets.
* [ ]  Visitors with unescorted access to the restricted areas or critical assets.

|  | Option 1 | Option 2 | Option 3 | Option 4 | Other |
| --- | --- | --- | --- | --- | --- |
| Check if utilizing  |[x] [ ] [ ] [ ]   |
| Define to which individuals the option applies | All facility employees, delivery drivers, and contractors |  |  |  |  |

[x]  The facility has designated and trained an individual or individual(s) (to include third parties) responsible for RBPS 12(iv).

[x]  The facility certifies that all affected individuals will be covered by one or more of the options listed above, and the facility will comply with RBPS 12(iv).

[x]  The facility has identified how it will safeguard information about affected individuals that is obtained from the CSAT Personnel Surety Program application.

[x]  The facility certifies that it will comply with the timeframe required for the implementation of the CFATS RBPS 12(iv) Personnel Surety Program, according to their facility’s Tier level.

### Option 1

Select “Yes” or “No” to indicate whether or not the facility affirms that notice has been or will be provided to the affected individuals whose information is being submitted under Option 1 which (1) notifies those individuals that their information is being submitted to DHS for vetting against the Terrorist Screening Database, and in some cases additional information may be requested and submitted in order to resolve a potential match; (2) instructs those individuals how to access their information; (3) instructs those individuals how to correct their information; and (4) instructs those individuals on procedures available to them for redress if they believe their information has been improperly matched by the Department to information contained in the Terrorist Screening Database.

* [x]  Yes [ ]  No

Does the facility plan to notify DHS via CSAT when an affected individual no longer has access to restricted areas or critical assets?

* [x]  Yes [ ]  No

Additional Comments or Details:

|  |
| --- |
| The facility will indicate the date the affected individuals will no longer have access when initially  |
| submitting the record by including the date of the facility access credential in the CSAT PSP data |
| field. For contractors, the facility will indicate the date the affected individuals will no longer have |
| access when initially submitting the record by indicating the end of the calendar year after the |
| contract period of performance expires. The facility will update the records of all affected individuals |
| annually or if the contract period of performance is modified. |
|  |
|  |
|  |
|  |
|  |

## RBPS 12(iv) SAMPLE: Option 1 and Option 2

The facility has the following types of affected individuals:

* [x]  Facility personnel (e.g., employees, contractors) with access to the restricted areas or critical assets.
* [x]  Visitors with unescorted access to the restricted areas or critical assets.

|  | Option 1 | Option 2 | Option 3 | Option 4 | Other |
| --- | --- | --- | --- | --- | --- |
| Check if utilizing  |[x] [x] [ ] [ ]   |
| Define to which individuals the option applies | All facility employees | Delivery drivers and contractors |  |  |  |

[x]  The facility has designated and trained an individual or individual(s) (to include third parties) responsible for RBPS 12(iv).

[x]  The facility certifies that all affected individuals will be covered by one or more of the options listed above, and the facility will comply with RBPS 12(iv).

[x]  The facility has identified how it will safeguard information about affected individuals that is obtained from the CSAT Personnel Surety Program application.

[x]  The facility certifies that it will comply with the timeframe required for the implementation of the CFATS RBPS 12(iv) Personnel Surety Program, according to their facility’s Tier level.

### Option 1

Select "Yes" or "No" to indicate whether or not the facility affirms that notice has been or will be provided to the affected individuals whose information is being submitted under Option 1 which (1) notifies those individuals that their information is being submitted to DHS for vetting against the Terrorist Screening Database, and in some cases additional information may be requested and submitted in order to resolve a potential match; (2) instructs those individuals how to access their information; (3) instructs those individuals how to correct their information; and (4) instructs those individuals on procedures available to them for redress if they believe their information has been improperly matched by the Department to information contained in the Terrorist Screening Database.

* [x]  Yes [ ]  No

Does the facility plan to notify DHS via CSAT when an affected individual no longer has access to restricted areas or critical assets?

* [x]  Yes [ ]  No

Additional Comments or Details:

|  |
| --- |
| For affected individuals, the facility will update the records about affected individuals within CSAT  |
| PSP annually to indicate when they no longer have access to the critical assets. The facility will also  |
| update and correct any other information it has become aware of (e.g., name changes). |
|  |
| For contractors, the facility will indicate the date the affected individuals will no longer have access  |
| when initially submitting the record by including the end of the calendar year after the  |
| contract period of performance expires in the CSAT PSP data field. The facility will update the records |
| of such affected individuals within CSAT PSP if the contract period of performance is modified. |

### Option 2

Select "Yes" or "No" to indicate whether or not the facility affirms that notice has been or will be provided to the affected individuals whose information is being submitted under Option 2 which (1) notifies those individuals that their information is being submitted to DHS for vetting against the Terrorist Screening Database, and in some cases, additional information may be requested and submitted in order to resolve a potential match; (2) instructs those individuals how to access their information; (3) instructs those individuals how to correct their information; and (4) instructs those individuals on procedures available to them for redress if they believe their information has been improperly matched by the Department to information contained in the Terrorist Screening Database.

* [x]  Yes [ ]  No

Provide additional comments/descriptions of this notice and how it will be provided to affected individuals.

|  |
| --- |
| The facility will use the DHS template to provide notice to all affected individuals. |
|  |
|  |

Indicate which vetting programs are used:

|  |
| --- |
| Transportation Worker Identification Credential (TWIC®) |

Types of facility personnel or unescorted visitors utilizing this program:

|  |
| --- |
| All delivery drivers and contractors |

What will the facility do if DHS is unable to verify an affected individual’s enrollment in another Department TSDB vetting program?

|  |
| --- |
| Revert to Option 1 for the individual |

What will be the timeframe for follow-on action if DHS is unable to verify an affected individual’s enrollment in another Department TSDB vetting program?

* + [ ]  0-1 days
	+ [x]  1-2 days
	+ [ ]  2-3 days
	+ [ ]  3-4 days

## RBPS 12(iv) SAMPLE: Option 3 and 4

The facility has the following types of affected individuals.

* [x]  Facility personnel (e.g., employees, contractors) with access to the restricted areas or critical assets.
* [x]  Visitors with unescorted access to the restricted areas or critical assets.

|  | Option 1 | Option 2 | Option 3 | Option 4 | Other |
| --- | --- | --- | --- | --- | --- |
| Check if utilizing  |[x] [ ] [x] [x]   |
| Define to which individuals the option applies | Employees with access to critical assets without TWIC |  | Employees with access to critical assets that possess TWIC | Delivery Drivers |  |

[x]  The facility has designated and trained an individual or individual(s) (to include third parties) responsible for RBPS 12(iv).

[x]  The facility certifies that all affected individuals will be covered by one or more of the options listed above, and the facility will comply with RBPS 12(iv).

[x]  The facility has identified how it will safeguard information about affected individuals that is obtained from the CSAT Personnel Surety Program application.

[x]  The facility certifies that it will comply with the timeframe required for the implementation of the CFATS RBPS 12(iv) Personnel Surety Program, according to their facility’s Tier level.

### Option 3

Will the facility provide notice to the affected individuals under Option 3 which (1) notifies the affected individual that their credential or document will be used for compliance with 6 CFR § 27.230 (a)(12)(iv); (2) informs them that no additional action will be taken if the credential is successful verified; and (3) notifies them of the facility’s actions should the credential or document not be successfully verified?

* [x]  Yes [ ]  No

If yes, provide additional comments/descriptions of this notice and how it will be provided to affected individuals.

|  |
| --- |
| The facility will use the DHS template to provide notice to all affected individuals. |
|  |

Has the facility designated and trained an individual or individual(s) to verify TWICs through use of the electronic reader or manually through the use of Cancel Credential List (CCL) and Credential Revocation List (CRL)?

* [x]  Yes [ ]  No

Indicate the frequency that the facility will revalidate TWIC credentials to ensure they are active.

* [ ]  Each visit/each entry
* [ ]  Once a week
* [ ]  Once a month
* [ ]  Other

Comments:

|  |
| --- |
| Delivery Drivers arrive at unknown and unscheduled times and are not issued keys, a key fob, or  |
| badge.TWICs are verified using the TWIC® ADVISR™ mobile application every time the affected  |
| individuals present themselves for access.[[1]](#footnote-1) |
| * The facility will validate a TWIC® by visually checking the expiration date and scan the card
 |
| identification number (CIN) from a TWIC card and input the card’s expiration date to  |
| determine if the TWIC® is canceled on the Visual Canceled Card List (VCCL).[[2]](#footnote-2) |
| * The facility will conduct identity verification by comparing the TWIC’s facial biometric
 |
| photograph to the individual presenting the TWIC®. |
| * The facility will use the TWIC® Authentication Guide to verify the TWIC’s authenticity.
 |

Does the facility have procedures that describe what mode or modes (i.e., which setting on the TWIC Reader) will be used when verifying and validating the TWIC of an affected individual?

* [x]  Yes [ ]  No

Additional Information:

|  |
| --- |
| The facility will use at a minimum “Mode 3 - Cardholder Unique Identifier (CHUID) Verification +  |
| Biometric User Authentication” prior to issuing keys, a key fob, or badge. |

Will the facility conduct a visual verification of TWICs along with the electronic verification?

* [x]  Yes [ ]  No

If yes, check all that apply:

* [x]  Comparing a picture on the credential or document to the affected individual in possession of the credential or document
* [x]  Comparing any physical characteristics listed on the credential or document (e.g., height, hair color, eye color) with the physical appearance of the affected individual in possession of the document or credential
* [x]  Checking for tampering
* [x]  Reviewing both sides of the credential or document and checking for the appropriate stock/credential material
* [x]  Checking for an expiration date
* [x]  Checking for any insignia, watermark, hologram, signature or other unique feature

What will the facility do if an affected individual’s TWIC cannot be verified or if the TWIC reader is not functioning properly?

|  |
| --- |
| The facility will not allow access to critical assets and restricted area until the individual’s TWIC® can  |
| be initially verified. |

What will be the timeframe for follow-on action due to the inability to verify credentials?

* [x]  0-1 days
* [ ]  1-2 days
* [ ]  2-3 days
* [ ]  3-4 days

### Option 4

Will the facility provide notice to the affected individuals under Option 4 which (1) notifies the affected individual that their credential or document will be used for compliance with 6 CFR § 27.230 (a)(12)(iv); (2) informs them that no additional action will be taken if the credential is successful verified; and (3) notifies them of the facility’s actions should the credential or document not be successfully verified?

* [x]  Yes [ ]  No

If yes, provide additional comments/descriptions of this notice and how it will be provided to affected individuals.

|  |
| --- |
| The facility has developed privacy notices to inform each affected individual of the above  |
| information. |

Has the facility designated and trained an individual or individual(s) to verify credentials or documents?

* [x]  Yes [ ]  No

Does the facility maintain a policy outlining which credentials or documents are acceptable for visual verification?

* [x]  Yes [ ]  No

Which credentials or documents will be accepted by the facility?

Credential or document:

|  |
| --- |
| HazMat Endorsement (HME) Program |

Types of facility personnel or unescorted visitors utilizing this credential:

|  |
| --- |
| All facility employees |

Credential or document:

|  |
| --- |
| TWIC® |

Types of facility personnel or unescorted visitors utilizing this credential:

|  |
| --- |
| All facility employees |

Which credentials or documents will not be accepted by the facility?

Credential or documents:

|  |
| --- |
| All others |

What methods will be utilized to visually verify credentials or documents accepted under visual verification? Check all that apply.

* [x]  Comparing a picture on the credential or document to the affected individual in possession of the credential or document;
* [x]  Comparing any physical characteristics listed on the credential or document (e.g. height, hair color, eye color) with the physical appearance of the affected individual in possession or the document or credential;
* [x]  Checking for tampering;
* [x]  Reviewing both sides of the credential or document and checking for the appropriate stock/credential material;
* [x]  Checking for an expiration date; and
* [x]  Checking for any insignia, watermark, hologram, signature or other unique feature.

Describe:

|  |
| --- |
| Security guards will be trained to check credential utilizing the above methods  |

What will the facility do if it is unable to visually verify an affected individual’s credential or document, the credential or document fails visual verification, or the credential or document appears invalid, expired, or fraudulent?

|  |
| --- |
| The affected individual will not be allowed access to critical assets. |

1. To date, DHS has not received any Site Security Plans selecting Option 3 and therefore the sample answers have been provided as an example but is not based on lessons learned or best practices. [↑](#footnote-ref-1)
2. The VCCL check may be performed by downloading the VCCL to a device equipped to process the VCCL (or processed by an access control system) or leveraging validation solutions developed by TSA or another entity (where available).

The TWIC® Advanced Digital Visual Inspection Solution for Revocation (ADVISR™) mobile applicable is available in beta on Android and iOS operating systems. [↑](#footnote-ref-2)