Chemical Security Assessment Tool (CSAT) Personnel Surety Program Application User Manual

March 1, 2016

Homeland Security

Table of Contents

Table of Figures

1. Introduction

The Chemical Facility Anti-Terrorism Standards (CFATS) program fosters security at America's highest risk chemical facilities. Working with the Department, facilities regulated under CFATS develop and implement Site Security Plans (SSP) and Alternative Security Programs (ASP) to address the 18 Risk-Based Performance Standards (RBPS). Included within these is RBPS 12(iv), which is designed to ensure certain individuals at high-risk chemical facilities are checked for terrorist ties. RBPS 12(iv) is currently only applicable to those CFATS regulated facilities which have been assigned as a Tier-1 or Tier-2 facility. The Department has developed four options in order to comply with the Personnel Surety Program. Information on the four options can be found at https://federalregister.gov/a/2015-31625.

This document is the user manual for the CFATS Chemical Security Assessment Tool (CSAT) Personnel Surety Program (PSP) application, an information-gathering application developed by the U.S. Department of Homeland Security (DHS) to assist Tier-1 and Tier-2 high-risk chemical facilities to comply with their SSP or ASP by submitting information about affected individuals who have or who are seeking access to restricted areas or critical assets. This information may be submitted under Option 1 for vetting against the Terrorist Screening Database (TSDB), or under Option 2 for electronic verification of an affected individual's enrollment in the Transportation Worker Identification Credential (TWIC) Program, the Hazardous Materials Endorsement (HME), or the Trusted Traveler Programs: NEXUS, Free and Secure Trade (FAST), Global Entry, and Secure Electronic Network for Travelers Rapid Inspection (SENTRI). Options 3 and 4 do not include submission of information to the Department and therefore, are not covered by this User Manual.

This user manual describes how a covered chemical facility Authorizer can utilize the PSP application to (1) establish a user structure; (2) manage the submission of records about affected individuals; (3) verify an affected individual's enrollment in TWIC Program, HME Program, or one of the Trusted Traveler Programs; and (4) view alerts about records of affected individuals submitted to the Department. Additional information about the CFATS PSP may be found at www.dhs.gov/chemicalsecurity. The Department has provided additional information pertaining to options for compliance, definitions, and other information related to the implementation of the CFATS PSP through the Implementation Notice that can be found at https://federalregister.gov/a/2015-31625.

2. Privacy

Information about affected individuals submitted to the Department and/or obtained from the CSAT PSP application is a government record and subject to the Privacy Act of 1974. This information is considered to be Sensitive Personally Identifiable Information (SPII). If SPII is lost, compromised, or disclosed without authorization, it could result in substantial harm, embarrassment, or unfairness to an affected individual. More information about SPII can be found in the DHS Handbook for Safeguarding Sensitive Personal Identifiable Information at http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf. Information collected or retained by the facility that has not been submitted to the Department and facility-generated copies of information that have been submitted to the Department are not considered government records and therefore are not covered under the Privacy Act of 1974, 5 U.S.C. § 552a.

3. Getting Started

The Department will grant the CSAT Authorizer access to the CSAT PSP application when (1) the Department authorizes or approves a SSP or ASP that does not have an RBPS 12(iv) condition, and (2) the facility has opted to implement Option 1 or Option 2 in its SSP or ASP. The CSAT Authorizer will have the ability to manage access for additional users who may assist in submitting information about affected individuals.

3.1 Logging In

After authentication of the username and password, a user will be directed to the Rules of Behavior (ROB) screen. The user will be logged into the PSP application after clicking the 'Accept' button. The ROB may be viewed in Attachment 3 of the May 2014 Privacy Impact Assessment (PIA) Update for the CFATS PSP that can be found at http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-cfatsps-may2014_0.pdf.

3.2 Application Menu

The CSAT PSP application has five tabs. Two of the five tabs are visible only to the Authorizer. The five tabs are:

- Affected Individuals Option 1 (accessible by all users): Allows users to (a) access affected individual records submitted under Option 1 and/or (b) input affected individual records under Option 1 (one at a time or via the Bulk Upload process).
- Affected Individuals Option 2 (accessible by all users): Allows users to (a) access affected individual records submitted under Option 2 and/or (b) input affected individual records under Option 2 (one at a time or via the Bulk Upload process).
- Submitters & Groups (accessible by Authorizer only): Allows the Authorizer to create groups and to assign PSP Submitters to groups. Under this tab, an Authorizer may also initiate the registration process for individuals without a CSAT user role.
- User Defined Fields (accessible by Authorizer only): Allows the Authorizer to create customized fields for storing any information desired by the Authorizer to assist with the management of affected individual records.
- Manage Alerts (accessible by all users): Allows users to configure alerts and/or monitor changes in the status of a record about an affected individual.

3.3 User Roles

The Authorizer, when accessing the PSP application, can:

- View, edit, and input information about affected individuals under Option 1 or Option 2
- Create/manage alerts
- Initiate the user registration process for individuals without an existing CSAT user role and assign them PSP Submitter rights
- Assign an existing CSAT user PSP Submitter rights
- Create/manage groups
- Create/manage User Defined Fields (UDF)

The PSP Submitter user role is a new user role within CSAT. This user role should not be confused with the more general Submitter user role applicable to those who submit information to the Department in other CSAT applications. The PSP Submitter role is assigned by the Authorizer. PSP Submitters can:

- View, edit, and input information about affected individuals under Option 1 or Option 2
- Create/manage alerts

PSP Submitters are designated individuals who may submit information about affected individuals on behalf of the Authorizer. Some examples of PSP Submitters are (1) an employee of the facility, (2) an employee or contractor of a corporation which owns the facility, or (3) a third-party contractor performing work on behalf of the facility.

User Roles	Can create/ assign/ manage groups	Can create PSP Submitters and assign them to groups	Can view data about affected individuals	Can input data	Can edit data	Can submit data
Authorizer	Yes	Yes	Yes	Yes	Yes	Yes
PSP Submitter	No	No	Yes*	Yes	Yes*	Yes

Table 1: Snapshot of User Roles and Rights

*Visibility of affected individual records is dependent on the user structure established through groups. PSP Submitters may only view and edit those records under their assigned purview setup by the Authorizer.

4. Submitting Information About Affected Individuals

4.1 Submitting Information About Affected Individuals via Option 1

Option 1 (Direct Vetting), mandatory data fields are:

1. U.S. Person (U.S. Citizens and Nationals as well as U.S. Lawful Permanent Residents)
   a. Full Name
   b. Date of Birth
   c. Citizenship or Gender
2. Non-U.S. Persons
   a. Full Name
   b. Date of Birth
   c. Citizenship
   d. Passport Information or Alien Registration Number

To reduce the likelihood of false positives in matching against records in the Federal Government’s consolidated and integrated terrorist watch list and to assist users with record management, the Authorizer and PSP Submitters may submit the following optional information about affected individuals to the Department.

The optional data fields are:

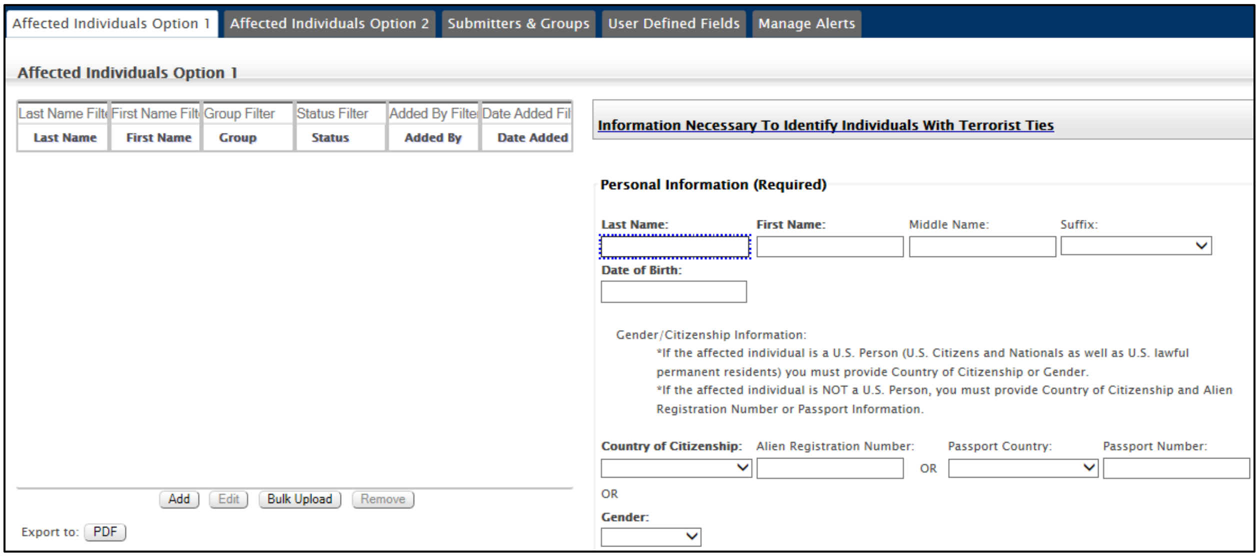
1. Date Affected Individual Will No Longer Have Access (The date must be after the date of submission but less than 10 years)
2. Aliases
3. Gender (for non-U.S. Persons)
4. Place of Birth

5. Redress Number
6. UDFs (only when created by the Authorizer)

Please see Appendix F for policy requirements about the submission of an affected individual's data and discussion about the use of optional data fields.

To submit information about affected individuals via Option 1, follow the instructions below:

1. Click on 'Affected Individuals Option 1' tab. On the bottom left side of the page click 'Add.'
2. On the right side of the screen, fill in the information and click 'Submit Record to DHS.'
3. Read the 'Affirmation of Information Veracity' and click 'Ok.'
4. The affected individual information is added to the affected individuals list on the left side of the page with a 'Submitted' status.



Affected Individuals Option 1

Last Name Filt	First Name Filt	Group Filter	Status Filter	Added By Filte	Date Added Fil
Last Name	First Name	Group	Status	Added By	Date Added

Information Necessary To Identify Individuals With Terrorist Ties

Personal Information (Required)

Last Name: First Name: Middle Name: Suffix:

Date of Birth:

Gender/Citizenship Information:
*If the affected individual is a U.S. Person (U.S. Citizens and Nationals as well as U.S. lawful permanent residents) you must provide Country of Citizenship or Gender.
*If the affected individual is NOT a U.S. Person, you must provide Country of Citizenship and Alien Registration Number or Passport Information.

Country of Citizenship: Alien Registration Number: OR Passport Country: Passport Number:

OR

Gender:

Figure 1: Screenshot of CSAT PSP application when submitting information about an affected individual under Option 1

4.2 Submitting Information About Affected Individuals via Option 2

Option 2 (Verification of Enrollment), mandatory data fields are:

1. Full Name
2. Date of Birth
3. Program-specific information or credential information:
   a. TWIC
      i. TWIC Agency Serial Number (How to obtain the TWIC Agency Serial Number visually and electronically can be found in Appendix E.)
      ii. Expiration Date Displayed on TWIC
   b. HME
      i. Commercial Driver's License Number
      ii. Expiration Date Displayed on the Commercial Driver's License
      iii. Issuing State of Commercial Driver's License Number
   c. Trusted Traveler Program

i. Pass ID Number (See Figure 6 for an example of a Trusted Traveler Program Pass ID.)
ii. Expiration Date Displayed on the Trusted Traveler Program Credential (Trusted Traveler members who do not have a card can find their PASS ID, including the expiration date and the name they used to enroll with the trusted Traveler program, on their online Global Entry (GOES) account at http://www.cbp.gov/travel/trusted-traveler-programs)

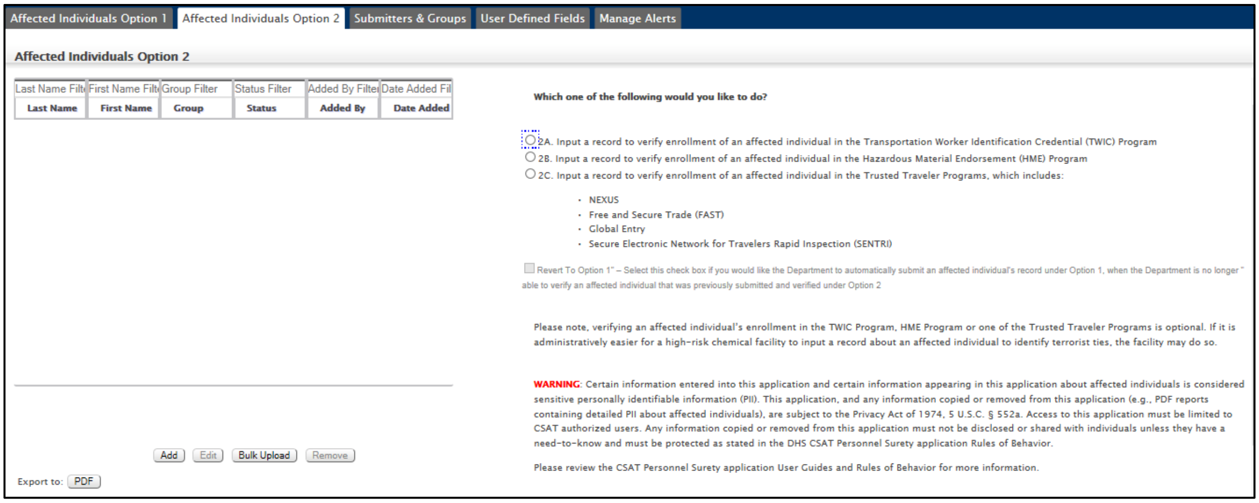
To reduce the potential for misidentification, and to assist users with record management, the Authorizer and PSP Submitters may submit the following optional information about affected individuals to the Department. The optional fields are:

1. Date Affected Individual will no Longer Have Access (The date must be after the date of submission but less than 10 years.)
2. Aliases
3. Gender
4. Place of Birth
5. Citizenship
6. UDFs (only when created by the Authorizer)

Please see Appendix F for policy requirements about the submission of an affected individual's data and discussion about the use of optional data fields.

To submit information about affected individuals via Option 2, follow the instructions below:

1. Click on 'Affected Individuals Option 2' tab. On the bottom left side of the page click 'Add.'
2. On the right side of the screen, select the program or credential type. Check the 'Revert To Option 1' checkbox if you would like the Department to automatically submit an affected individual's record under Option 1 when the Department is either (1) unable to verify an affected individual's enrollment or (2) no longer able to verify an affected individual's enrollment. On the bottom of the page click 'Continue.'
3. Fill in the information for the program and click 'Submit Record to DHS.'
4. Read the 'Affirmation of Information Veracity' and click 'Ok.'
5. The affected individual information is added to the affected individuals' list on the left side of the page with 'Verification Pending' status.



Affected Individuals Option 2

Last Name Filt	First Name Filt	Group Filter	Status Filter	Added By Filter	Date Added Fil
Last Name	First Name	Group	Status	Added By	Date Added

Which one of the following would you like to do?

○ 2A. Input a record to verify enrollment of an affected individual in the Transportation Worker Identification Credential (TWIC) Program
○ 2B. Input a record to verify enrollment of an affected individual in the Hazardous Material Endorsement (HME) Program
○ 2C. Input a record to verify enrollment of an affected individual in the Trusted Traveler Programs, which includes:

- NEXUS
- Free and Secure Trade (FAST)
- Global Entry
- Secure Electronic Network for Travelers Rapid Inspection (SENTRI)

□ Revert To Option 1" – Select this check box if you would like the Department to automatically submit an affected individual's record under Option 1, when the Department is no longer " able to verify an affected individual that was previously submitted and verified under Option 2

Please note, verifying an affected individual's enrollment in the TWIC Program, HME Program or one of the Trusted Traveler Programs is optional. If it is administratively easier for a high-risk chemical facility to input a record about an affected individual to identify terrorist ties, the facility may do so.

WARNING: Certain information entered into this application and certain information appearing in this application about affected individuals is considered sensitive personally identifiable information (PII). This application, and any information copied or removed from this application (e.g., PDF reports containing detailed PII about affected individuals), are subject to the Privacy Act of 1974, 5 U.S.C. § 552a. Access to this application must be limited to CSAT authorized users. Any information copied or removed from this application must not be disclosed or shared with individuals unless they have a need-to-know and must be protected as stated in the DHS CSAT Personnel Surety application Rules of Behavior.

Please review the CSAT Personnel Surety application User Guides and Rules of Behavior for more information.

Figure 2: Screenshot of CSAT PSP application when submitting information about an affected individual under Option 2

Option 2 provides an option to revert back to Option 1. The purpose of the 'Revert to Option 1' checkbox is to reduce the burden on facilities. In the event the record either cannot be verified or is later unable to be verified, and the 'Revert to Option 1' has been selected, the PSP application will automatically submit the record under Option 1 if either of the following two situations occurs:

- The record submitted under Option 2 has a change in status from 'Verification Pending' to 'Not Verified.'
- The record submitted under Option 2 has a change in status from 'Verified' to 'No Longer Verified.'

Please see section 4.5 for more information on status descriptions.

In either scenario, the CSAT PSP application will automatically submit the record under Option 1 and change the record's status to 'Submitted.' The record will then appear in the 'Affected Individuals Option 1' tab.

To utilize 'Revert to Option 1' the PSP Submitter must check the 'Revert to Option 1' checkbox. When a PSP Submitter opts to use this feature, the CSAT PSP application will collect the required information necessary to verify enrollment under Option 2 and any additional data fields necessary to meet the minimum data requirements for submitting a record about an affected individual under Option 1.

4.3 Steps for Bulk Upload (Option 1 and Option 2)

Bulk Upload is a capability that allows a user to submit information about more than one affected individual at the same time for both Option 1 and Option 2 submissions. The same spreadsheet may contain both Option 1 and Option 2 records.

To download a copy of the Bulk Upload template follow the instructions below:

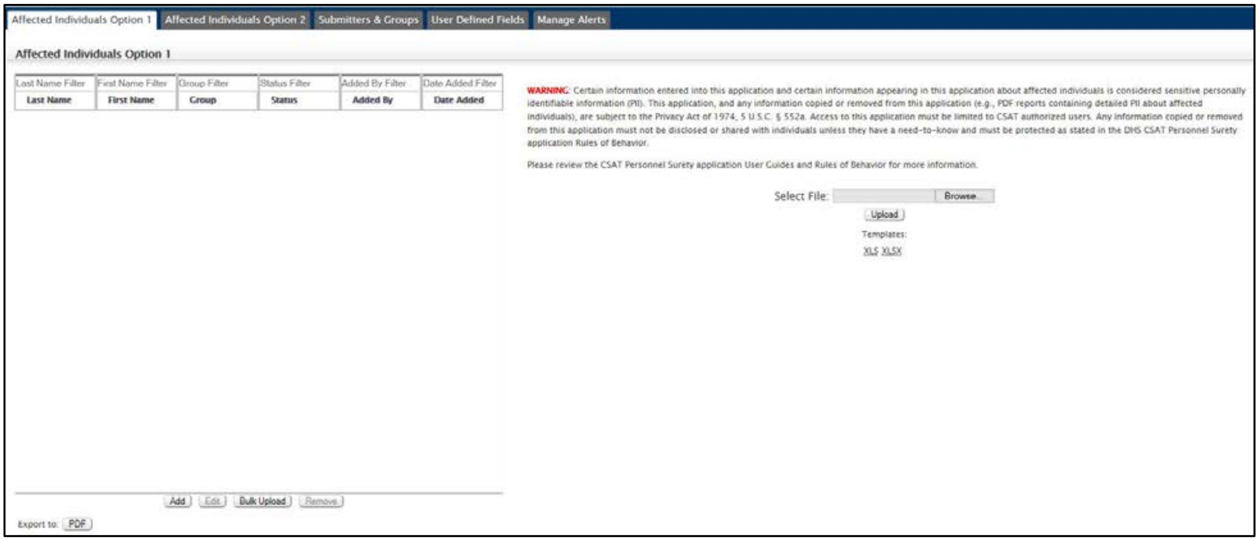
1. Select either 'Affected Individuals Option 1' tab or 'Affected Individuals Option 2' tab.
2. Click the 'Bulk Upload' button at the bottom left of the screen.
3. Download one of the two templates (XLS or XLSX).

To submit a Bulk Upload, follow the instructions below:

1. Input affected individual data into the template and save the document. Information about the specific data fields and applicable parameters may be found in Appendix B.
2. Select either ‘Affected Individuals Option 1’ tab or ‘Affected Individuals Option 2’ tab.
3. Click the ‘Bulk Upload’ button at the bottom left of the screen.
4. Click ‘Browse’ and select the Bulk Upload template that contains information about affected individuals, from the saved location on the user’s computer.
5. Click ‘Upload.’
6. Read the ‘Affirmation of Information Veracity’ and click ‘Ok.’
7. The affected individuals information is added to the affected individuals list on the left side of the Option 1 page with the ‘Submitted’ status or Option 2 page with ‘Verification Pending’ status.

Upon submission of the Bulk Upload template, the CSAT PSP application will display the results on the submission screen and in an email to the PSP Submitter. The results displayed will include the number of records successfully uploaded (i.e., submitted) and records with errors. The CSAT PSP application will display the row number and the reason for the error (e.g., no date of birth was provided). Records identified with errors must be resubmitted by the PSP Submitter after correction. The CSAT PSP application will also identify those records that are duplicates and were not accepted. These records do not require additional attention because an identical record already exists in the group to which the PSP Submitter belongs.

Note: The Department has developed a Bulk Upload template to be used in conjunction with the Bulk Upload capability. The Department developed the template so Authorizers and PSP Submitters can reduce the likelihood of receiving CSAT processing errors generated by incompatible formats or coding.



WARNING: Certain information entered into this application and certain information appearing in this application about affected individuals is considered sensitive personally identifiable information (PII). This application, and any information copied or removed from this application (e.g., PDF reports containing detailed PII about affected individuals), are subject to the Privacy Act of 1974, 5 U.S.C. § 552a. Access to this application must be limited to CSAT authorized users. Any information copied or removed from this application must not be disclosed or shared with individuals unless they have a need-to-know and must be protected as stated in the DHS CSAT Personnel Surety application Rules of Behavior.

Please review the CSAT Personnel Surety application User Guides and Rules of Behavior for more information.

Figure 3: Screenshot of CSAT PSP application when submitting information via Bulk Upload about affected individuals

4.4 Indicating an Affected Individual No Longer Has Access

An Authorizer or PSP Submitter may at any time notify the Department that an affected individual no longer has access to restricted areas or critical assets. To notify the Department that an affected individual no longer has access to restricted areas or critical assets, follow the instructions below:

1. Select the 'Affected Individuals Option 1' tab or 'Affected Individuals Option 2' tab containing the affected individual's record.
2. Select the record.
3. Click the 'Remove' button. A warning box will pop up requesting the user to validate the removal.

Appendix F contains a summary of the various ways a user may notify the Department that an affected individual no longer has access, as well as several examples an Authorizer or its designees may wish to consider.

When the Department is notified that an affected individual no longer has access to restricted areas or critical assets, the record will no longer be displayed. The Department will also (1) stop vetting the affected individual in accordance with the record retention schedule for the CFATS PSP[1] if the affected individual was submitted under Option 1, or (2) stop verifying the affected individual's enrollment in other DHS programs.

4.5 Sorting and Viewing Record Status after Submission

The Authorizer and PSP Submitters may sort records about affected individuals in the 'Affected Individuals Option 1' tab and 'Affected Individuals Option 2' tab. Records can be sorted in ascending or descending order by selecting the following headers: Last Name, First Name, Status, Added By, and Date Added. If you are an Authorizer, you may also sort by group. The Authorizer may export a pdf file of all records submitted under Option 1 and Option 2. Submitters may also export a pdf file but are limited to only the records within the group they are assigned. The pdf files are alphabetically sorted by last name.[2]

The Department assigns a status to records about affected individuals submitted under Option 1 and Option 2.

The Option 1 status is:

- 'Submitted' – The record has been submitted to the Department for vetting of terrorist ties

The Option 2 statuses are:

- 'Verification Pending' – The record has been submitted to the Department for verification of the affected individual's enrollment and the Department is in the process of verifying enrollment.
- 'Verified' – The Department has verified the affected individual's enrollment. When a

[1] The CFATS PSP Systems of Records Notice (SORN), available at https://www.federalregister.gov/articles/2014/05/19/2014-11431/privacy-act-of-1974-department-of-homeland-security-national-protection-and-programs-directorate-002#p-103, describes the record retention schedule.

[2] Exports of information from the CSAT PSP application contain SPII and are subject to the Privacy Act of 1974, 5 U.S.C. § 552a. Any exported document and any information copied or removed from it, (1) must not be disclosed or shared with individuals unless they have a need-to-know, and (2) must be protected as stated in the DHS CSAT PSP application ROB.

record is ‘Verified,’ the Department will display the projected date the facility may no longer rely on the affected individual’s participation in the other DHS programs for purposes of checking for terrorist ties to comply with RBPS 12(iv).

- ‘Not Verified’ – The Department was unable to verify the affected individual’s enrollment.
- ‘No Longer Verified’ – The Department is no longer able to verify the affected individual’s enrollment. This status occurs only when the previous status was ‘Verified.’ This change occurs as a result of the Department periodically re-verifying the affected individual’s participation in the TWIC, HME, or Trusted Traveler Program.

5. Manage Alerts

These alerts are utilized to inform the Authorizer and Submitters of the various changes to the status of a record about an affected individual. Alerts can be received through e-mail and as a notification upon logging in to the PSP application. The five alerts include:

1. Record – Submitted: This alert is triggered when a record is submitted under Option 1.
2. Record – Verified: This alert is triggered when a record submitted under Option 2 is verified by the Department.
3. Record – Not Verified: This alert is triggered when a record submitted under Option 2 was not verified by the Department.
4. Record – No Longer Verified: This alert is triggered when a record submitted under Option 2 is no longer able to be verified by the Department, after the record was previously verified by the Department.
5. Record – Verification Pending: This alert is triggered when a record is submitted under Option 2 and is pending verification by the Department.

If users elect to receive e-mail alerts, the Department will send one e-mail with all relevant alerts which may have occurred over the past day. The e-mail subject will be “Personnel Surety Program Alerts.”

6. Administration of Accounts – Authorizer Only

6.1 Assigning the PSP Submitter Role to Individuals with an Existing CSAT Account

An Authorizer can assign an existing CSAT user the PSP Submitter role by following the steps below:

1. Click on ‘Submitters & Groups’ tab.
2. Click ‘Add CSAT User’ button.
3. Fill in ‘CSAT User Name’ and ‘Phone Number.’ (The same phone number the user listed in “Manage My Account” in the CSAT system).
4. Click ‘Save New User.’ The user status is updated to ‘Sent.’

Once the Authorizer completes the steps above, an e-mail is automatically sent to the existing CSAT User notifying them they have been assigned PSP Submitter rights and have access to the PSP application.

6.2 Assigning the PSP Submitter Role to Individuals Without an Existing CSAT Account

An Authorizer may initiate the process to enable an individual who does not have a CSAT account to become a PSP Submitter by following the steps below:

1. Click the ‘Submitters & Groups’ tab
2. Click the ‘Add New User’ button.
3. Fill in ‘First Name,’ ‘Last Name,’ and E-mail Address.’
4. Click ‘Save New User.’ The user status is updated to ‘Sent.’

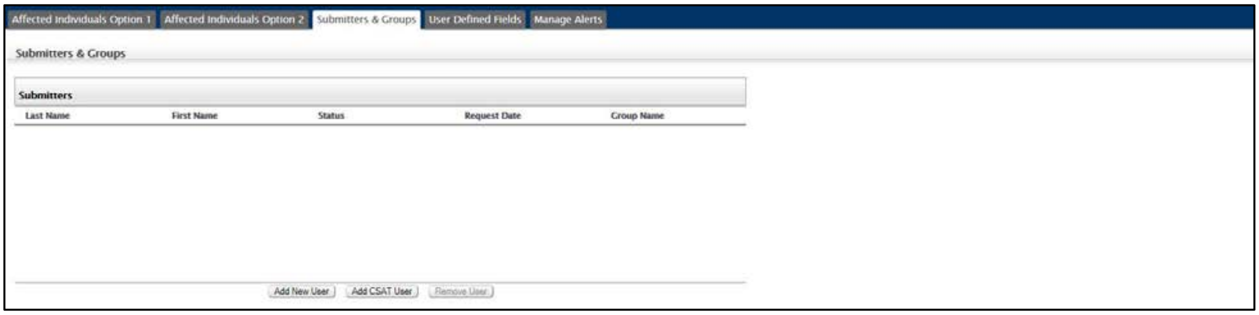
This initiates the user registration process; the new user is sent an e-mail with a link to the CSAT Registration Portal (the link is valid for 14 days and may only be used one time). The steps below must be followed in order to apply for a PSP Submitter role:

1. The new user follows the link provided and provides the information requested in the User Registration Portal.
2. The new user signs the document and then faxes or e-mails the form back to the CSAT Help Desk.
3. The new user receives an e-mail with login information once the account is approved by the Department.

6.3 Remove PSP Submitters Role

The Authorizer can at any time remove the PSP Submitter role by following the steps below:

1. Click on Submitters & Groups tab.
2. Click on the PSP Submitters name.
3. Click the ‘Remove User’ button.



Last Name	First Name	Status	Request Date	Group Name

Figure 4: Adding and Removing Users

6.4 Creating, Editing, Merging, and Removing Groups

The PSP application is designed to provide flexibility for Authorizers when managing who may submit, view, and update records about affected individuals under the Authorizer. Access to records about affected individuals in the PSP application is managed through groups created by the Authorizer and to which an Authorizer subsequently assigns PSP Submitters. A PSP Submitter assigned to a group may view and edit all records about affected individuals within that group. A PSP Submitter may only be assigned to one group under an Authorizer. The Authorizer cannot enter or edit records about affected individuals in those groups. The Authorizer only has the ability to edit records about affected individuals in the “Corporation” group. Please see section 6.5 for more information on “Corporation” group.

The record about an affected individual will be assigned to the group of the PSP Submitter. For example, when an Authorizer or PSP Submitter assigned to the "Corporation" group submits information about affected individuals, the record will be assigned to the "Corporation" group. Please see section 6.5 for more information on "Corporation" groups.

6.5 Privacy Considerations When Creating, Editing, and Removing Groups

When the Department initially grants the Authorizer access to the PSP application, a default group labeled "Corporation" is established. The Authorizer is automatically assigned to the default group and may not be assigned to a different group.

The Department expects an Authorizer will carefully consider the best group structure so information about affected individuals can be protected from unauthorized disclosure. Specifically, the Department expects the Authorizer will create one or more groups if needed so PSP Submitter(s) will (1) have access to only those records about affected individuals they should have access to, and (2) not have access to those records about affected individuals they should not. Several examples of how groups might be constructed to align with a facility's (or its designees') business operations are provided in Appendix C. It is also possible that the best group structure for some facilities may be to not create any additional groups at all and rely on the default "Corporation" group.

A new group is not required for each individual PSP Submitter. Multiple PSP Submitters can be assigned to a single group. However, a group must have at least one PSP Submitter assigned to it.

Note: An Authorizer may assign additional PSP Submitters to the "Corporation" group; however, the Department expects only employees of the corporation/facility to be assigned to the "Corporation" group. Any PSP Submitter assigned to the "Corporation" group will have access to all affected individual records submitted under the Authorizer's purview.

6.6 Steps to Create a Group

Groups are created to manage the purview of PSP Submitters who will be submitting information about affected individuals and to avoid inappropriate disclosure of SPII.

Steps an Authorizer must follow to create a group are:

1. Click the 'Submitters & Groups' tab.
2. Click the 'Create New Group' button.
3. Fill in 'Name' and 'Description.'
4. Click 'Save New Group.'

6.7 Steps to Edit a Group's Name or Description

Editing a group allows a user to change or correct the spelling of a group's name and change or add the description about the particular group being edited.

Steps an Authorizer must follow to edit a group are:

1. Click the 'Submitters & Groups' tab.
2. Select 'Group' in 'Groups' box.
3. Make edits to group name or group description.
4. Click 'Save Edits To Group.'

6.8 Steps to Merge a Group

This function is utilized to merge the records of affected individuals in a group into the default group labeled “Corporation.” Once this action is completed, the merged records about affected individuals will not be severable from other affected individual records in the “Corporation” group. Further, once this action is completed, only PSP Submitters assigned to the Corporation group and Authorizers will be able to view and edit the affected individual records going forward.

Steps an Authorizer must follow to merge a group are:

1. Click the ‘Submitters & Groups’ tab.
2. Select ‘Group’ in ‘Groups’ box.
3. Click the ‘Merge Group’ button.
4. Click ‘Ok’ to acknowledge the action.

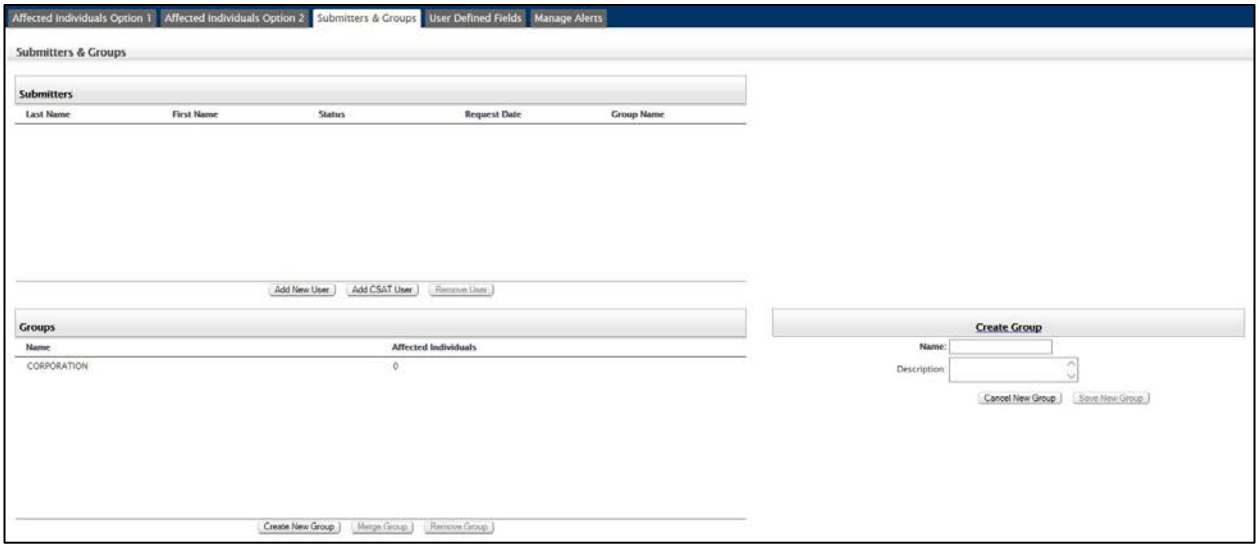
Note: Once a merge occurs, records cannot be unmerged.

6.9 Steps to Remove a Group

Removing a group will result in CSAT designating the records about affected individuals assigned for that group as “no longer having access.” Before removing a group a warning message will appear to validate the Authorizer’s intent to remove the group.

Steps an Authorizer must follow to remove a group are:

1. Click the ‘Submitters & Groups’ tab.
2. Select ‘Group’ in the ‘Groups’ box.
3. Click the ‘Remove Group’ button.
4. Click ‘Ok’ to acknowledge removal.



Submitters & Groups

Submitters

Last Name	First Name	Status	Request Date	Group Name

Groups

Name	Affected Individuals
CORPORATION	0

Create Group

Name:

Description:

Figure 5: Creating, Merging, and Removing a Group

7. User Defined Fields

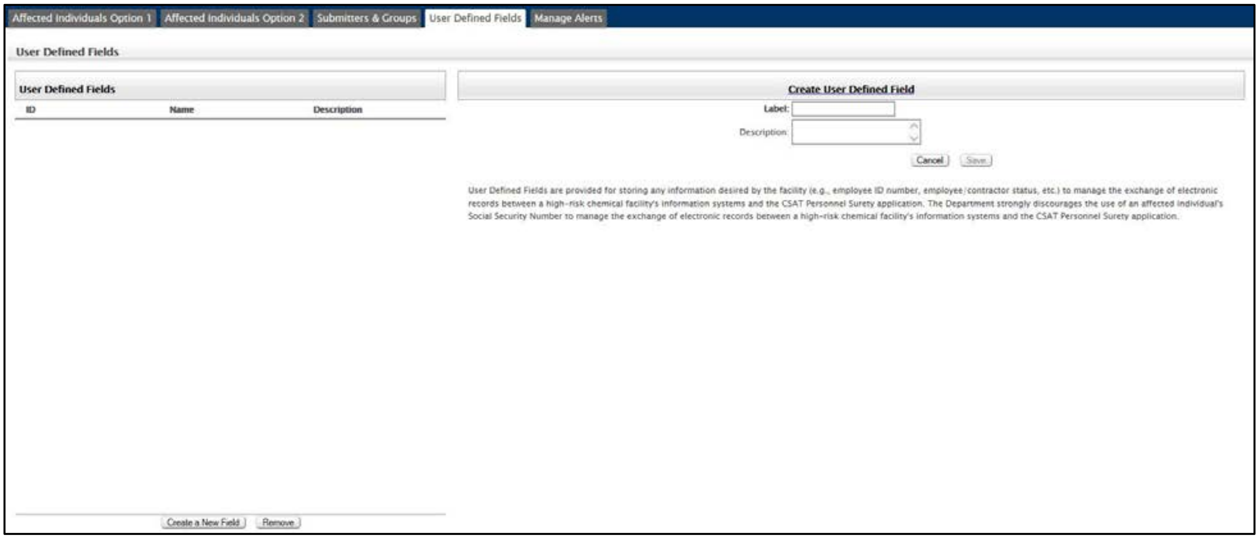
UDFs are provided for storing any information desired by the Authorizer to assist with the management of affected individual records. For example, an Authorizer may establish a UDF with the label ‘Contract Number or Name’ and require PSP Submitters of each group to enter the contract number or name for the contract under which the affected individual is being submitted. As an additional example, an Authorizer may establish a UDF with the label ‘Badge Number’ and require PSP Submitters of a group to input that data element when submitting information about affected individuals.

Only an Authorizer may create UDFs. Once created, PSP Submitters may include the appropriate data in the UDF when submitting a record about an affected individual. Authorizers can manage UDFs via the ‘User Defined Fields’ tab. Once created, UDFs are visible to the Authorizer in the ‘User Defined Fields’ tab and can be utilized within both Option 1 and Option 2 tabs.

Note: The Department strongly discourages the use of UDFs for storing an affected individual’s Social Security number or any other SPII.

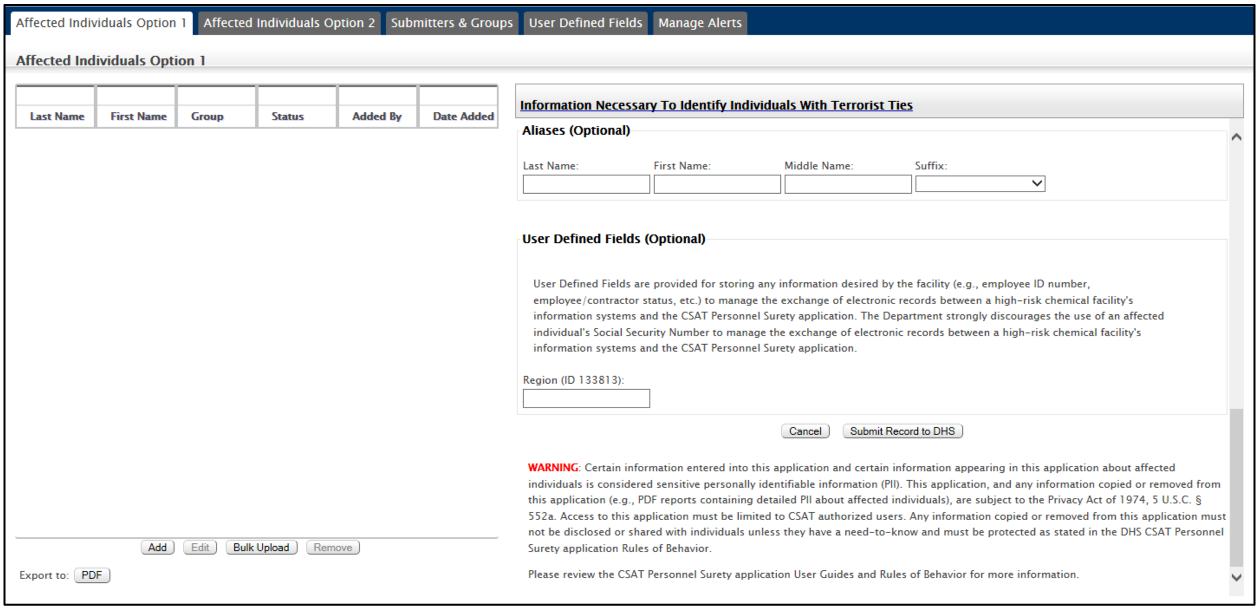
Steps an Authorizer must follow to create a UDF are:

1. Click on the ‘User Defined Fields’ tab.
2. Click ‘Create a New Field.’
3. Fill in ‘Label’ and ‘Description.’
4. Click ‘Save.’



User Defined Fields are provided for storing any information desired by the facility (e.g., employee ID number, employee/contractor status, etc.) to manage the exchange of electronic records between a high-risk chemical facility's information systems and the CSAT Personnel Surety application. The Department strongly discourages the use of an affected individual's Social Security Number to manage the exchange of electronic records between a high-risk chemical facility's information systems and the CSAT Personnel Surety application.

Figure 6: User Defined Fields Tab



Affected Individuals Option 1

Last Name	First Name	Group	Status	Added By	Date Added

Information Necessary To Identify Individuals With Terrorist Ties

Aliases (Optional)

Last Name: First Name: Middle Name: Suffix:

User Defined Fields (Optional)

User Defined Fields are provided for storing any information desired by the facility (e.g., employee ID number, employee/contractor status, etc.) to manage the exchange of electronic records between a high-risk chemical facility's information systems and the CSAT Personnel Surety application. The Department strongly discourages the use of an affected individual's Social Security Number to manage the exchange of electronic records between a high-risk chemical facility's information systems and the CSAT Personnel Surety application.

Region (ID 133813):

WARNING: Certain information entered into this application and certain information appearing in this application about affected individuals is considered sensitive personally identifiable information (PII). This application, and any information copied or removed from this application (e.g., PDF reports containing detailed PII about affected individuals), are subject to the Privacy Act of 1974, 5 U.S.C. § 552a. Access to this application must be limited to CSAT authorized users. Any information copied or removed from this application must not be disclosed or shared with individuals unless they have a need-to-know and must be protected as stated in the DHS CSAT Personnel Surety application Rules of Behavior.

Please review the CSAT Personnel Surety application User Guides and Rules of Behavior for more information.

Figure 7: User Defined Fields example for when a record is submitted under Option 1

8. Help

The CSAT Help Desk can be reached at CSAT@hq.dhs.gov or 866-323-2957 (toll free) between 8:30 a.m. and 5:00 p.m. (Eastern Time), Monday through Friday. The CSAT Help Desk is closed for Federal holidays.

Appendix A: Acronym List

ASN	Agency Serial Number
CDL	Commercial Driver’s License
CFATS	Chemical Facility Anti-Terrorism Standards
CIN	Card Image Number
CSAT	Chemical Security Assessment Tool
DHS	Department of Homeland Security
FAST	Free and Secure Trade
HME	Hazardous Materials Endorsement
IIN	Issuer Identification Number
PIV	Personal Identity Verification
PSP	Personnel Surety Program
RBPS	Risk-Based Performance Standards
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
SPII	Sensitive Personally Identifiable Information
SSP	Site Security Plan
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
UCI	Universal Credential Identification
UDF	User Defined Field

Appendix B: Bulk Upload

The Bulk Upload capability may process up to 10,000 affected individual records at a time. Bulk Upload files can be input in either an XLS or XLSX file. Every affected individual record submitted through the Bulk Upload process must contain data in the required fields, as seen in the tables below.

A single bulk upload may contain records in any combination of the below types:

- Option 1
- Option 2, and
- Option 2 (Revert to Option 1)

The tables below summarize the validation rules for each record within the Bulk Upload template. The validation rules are instructions for the IT system to ensure that a record about affected individuals is complete and able to be processed. However, just because a record about an affected individual is complete does not mean that the record has complied with the Department's submission requirements. Validation rules should not be confused with program policies. A PSP Submitter must ensure that the record complies with the Department's submission requirements as listed in the implementation notice and the policy statement provided in Appendix F.

> For example: The CSAT PSP application will accept as complete (i.e., system required fields are complete) a record about an affected individual under Option 1 which does not contain the affected individual's middle name because some affected individuals will not have a middle name. However, the Department requires a facility to submit an affected individual's full name (see the implementation notice and the policy statements in Appendix F). Thus, if a facility knows the affected individual has a middle name, the PSP Submitter is required to provide the middle name when submitting the affected individual's record to the Department.

Option 1 Bulk Upload - Field Mapping

Field	Description	Validation Rules	Format
Last Name	Affected individual's last name	Required	Non-null string Ex: Smith
First Name	Affected individual's first name	Required	Non-null string Ex: John
Middle Name	Affected individual's middle name	Optional	Non-null string Ex: Leon
Suffix	Affected individual's suffix	Optional	JR–Junior SR–Senior I–First II–Second III–Third IV–Fourth V–Fifth VI–Sixth VII–Seventh VIII–Eighth IX–Ninth X–Tenth

Option 1 Bulk Upload - Field Mapping			
Field	**Description**	**Validation Rules**	**Format**
Alias Last Name	Alternative last name	Required: Only when adding an alias(es) to the submission of an affected individual	Non-null string Ex: Jones
Alias First Name	Alternative first name	Required: Only when adding an alias(es) to the submission of an affected individual	Non-null string Ex: Sam
Alias Middle Name	Alternative middle name	Optional	Non-null string Ex: William
Alias Suffix	Alternative suffix	Optional	JR–Junior SR–Senior I–First II–Second III–Third IV–Fourth V–Fifth VI–Sixth VII–Seventh VIII–Eighth IX–Ninth X–Tenth
Date of Birth	Affected individual's date of birth	Required	MM/DD/YYYY
City of Birth	City of individual’s place of birth	Optional	There is no format for this field
Country of Birth	Country of individual’s place of birth	Optional	Must be ISO 3166 Alpha-3 code www.iso.org
Country of Citizenship	Individual's country of citizenship	Required: If the data field Gender is null	Must be ISO 3166 Alpha-3 code www.iso.org
Gender	Affected individual's gender	Required: If the data field Country of Citizenship is null	M–for Male F–for Female
Passport Country	Country issuing the passport	Required: If passport number is populated	Must be ISO 3166 Alpha-3 code www.iso.org
Passport Number	Passport number	Required: If passport country is populated	String between 1-20 characters Ex: P145827364
Redress Number	Redress number	Optional	7 digit number Ex: 4568219
Alien Registration	Alien registration number	Optional	An 8 or 9 digit number, can be optionally preceded with an ‘A’ or ‘a.’ The number cannot be all 0s or all 9s.
Custom Field ID	This field refers to the UDF ID number that is given after a UDF is created within the system	Optional: Must be a valid UDF that is accessible to the user on the Affected Individuals Record from within the system	Numbers only

Option 1 Bulk Upload - Field Mapping			
Field	**Description**	**Validation Rules**	**Format**
Value	Value of UDF. This is the information applicable to the field in the application.	Optional: Can be number, letters, and special characters. No longer than 200 characters.	There is no format for this field
No Access Date	Date when affected individual will no longer have access to restricted areas or critical assets at a facility. Upon the specified date, the affected individual will no longer be vetted.	Optional: The date must be greater than today and less than 10 years from now	MM/DD/YYYY

Option 2 Bulk Upload - Field Mapping (No Revert to Option 1)			
Field	**Description**	**Validation Rules**	**Format**
Last Name	Affected individual's last name	Required	Non-null string Ex: Smith
First Name	Affected individual's first name	Required	Non-null string Ex: John
Middle Name	Affected individual's middle name	Optional	Non-null string Ex: Leon
Suffix	Affected individual's suffix	Optional	JR–Junior SR–Senior I–First II–Second III–Third IV–Fourth V–Fifth VI–Sixth VII–Seventh VIII–Eighth IX–Ninth X–Tenth
Alias Last Name	Alternative last name	Required: Only when adding an alias(es) to the submission of an affected individual	Non-null string Ex: Jones
Alias First Name	Alternative first name	Required: Only when adding an alias(es) to the submission of an affected individual	Non-null string Ex: Sam
Alias Middle Name	Alternative middle name	Optional	Non-null string Ex: William
Alias Suffix	Alternative suffix	Optional	JR–Junior SR–Senior I–First II–Second III–Third IV–Fourth V–Fifth VI–Sixth VII–Seventh VIII–Eighth IX–Ninth X–Tenth
Date of Birth	Affected individual's date of birth	Required	MM/DD/YYYY
City of Birth	City of individual’s place of birth	Optional	There is no format for this field
Country of Birth	Country of individual’s place of birth	Optional	Must be ISO 3166 Alpha-3 code www.iso.org
Country of Citizenship	Individual's country of citizenship	Optional	Must be ISO 3166 Alpha-3 code www.iso.org
Gender	Affected individual's gender	Optional	M–for Male F–for Female

Option 2 Bulk Upload - Field Mapping (No Revert to Option 1)			
Field	**Description**	**Validation Rules**	**Format**
Alien Registration	Alien registration number	Optional	An 8 or 9 digit number, can be optionally preceded with an 'A' or 'a.' The number cannot be all 0s or all 9s.
Global ID *This is the number associated with the credential being vetted against	CDL Number	Required: Must be populated to verify enrollment in DHS program.	CDL Numbers vary across States based on formats
	TWIC Agency Serial Number		TWIC up to 9 digits
	PASS ID for FAST, Global Entry (GOES), NEXUS, and SENTRI		GOES, NEXUS, FAST and SENTRI are 9 digit numbers
Global Type *This is the type of enrollment program (TWIC, HME, Trusted Traveler)	Identifies the DHS Program being verified	Required: Enter one of the following values for each entry. Input of these values must be exact.	CDL/HME
			TWIC
			GOES, NEXUS, FAST, and SENTRI
CDL State	State abbreviation	Required: When DHS program selected is CDL/HME	Must be U.S. Postal Service Alpha-2 code www.usps.com
Expiration Date	Expiration date for the program being selected for verification. Commonly known as the credential's expiration date	Required: For all Option 2 submissions	MM/DD/YYYY
No Access Date	Date when affected individual will no longer have access to restricted areas or critical assets at a facility. Upon the specified date the affected individual's enrollment will no longer be verified.	Optional: The date must be greater than today and less than 10 years from now.	MM/DD/YYYY
Custom Field ID	This field refers to the UDF ID number that is given after a UDF is created within the system	Optional: Must be a valid UDF that is accessible to the user on the affected individual's record from within the system	Numbers only
Value	Value of UDF. This is the information applicable to the field for the user.	Optional: Can be number, letters, and special characters. No longer than 200 characters.	There is no format for this field
Revert to Option One	If this submission should not automatically revert to Option 1 under the system rules (refer to Section 4.1.2), then a value must be entered.	Required: All Option 2 submissions that are not 'Revert to Option 1' must contain a 'false' in the value for each affected individual submitted	'False' value only

Option 2 (Revert to Option 1) Bulk Upload - Field Mapping			
Field	**Description**	**Validation Rules**	**Format**
Last Name	Affected individual's last name	Required	Non-null string Ex: Smith
First Name	Affected individual's first name	Required	Non-null string Ex: John
Middle Name	Affected individual's middle name	Optional	Non-null string Ex: Leon
Suffix	Affected individual's suffix	Optional	JR–Junior SR–Senior I–First II–Second III–Third IV–Fourth V–Fifth VI–Sixth VII–Seventh VIII–Eighth IX–Ninth X–Tenth
Alias Last Name	Alternative last name	Required: Only when adding an alias(es) to the submission of an affected individual	Non-null string Ex: Jones
Alias First Name	Alternative first name	Required: Only when adding an alias(es) to the submission of an affected individual	Non-null string Ex: Sam
Alias Middle Name	Alternative middle name	Optional	Non-null string Ex: William
Alias Suffix	Alternative suffix	Optional	JR–Junior SR–Senior I–First II–Second III–Third IV–Fourth V–Fifth VI–Sixth VII–Seventh VIII–Eighth IX–Ninth X–Tenth
Date of Birth	Affected individual's date of birth	Required	MM/DD/YYYY
City of Birth	City of individual's place of birth	Optional	There is no format for this field
Country of Birth	Country of individual's place of birth	Optional	Must be ISO 3166 Alpha-3 code www.iso.org
Gender	Affected individual's gender	Required: If the data field Country of Citizenship is null	M–for Male F–for Female

Option 2 (Revert to Option 1) Bulk Upload - Field Mapping

Field	Description	Validation Rules	Format
Country of Citizenship	Individual's country of citizenship	Required: If the data field Gender is null	Must be ISO 3166 Alpha-3 code www.iso.org
Passport Country	Country issuing the passport	Required: If passport number is populated	Must be ISO 3166 Alpha-3 code www.iso.org
Passport Number	Passport number	Required: If passport country is populated	String between 1-20 characters Ex: P145827364
Redress Number	Redress number	Optional	7 digit number Ex: 4568219
Alien Registration	Alien registration number	Optional	An 8 or 9 digit number, can be optionally preceded with an 'A' or ‘a.’ The number cannot be all 0s or all 9s. Ex: 55548791
Global ID *This is the number associated with the credential being vetted against	CDL Number	Required: Must be populated to verify enrollment in DHS program	CDL Numbers vary across States based on formats
	TWIC Agency Serial Number		TWIC up to 9 digits
	PASS ID for FAST, Global Entry (GOES), NEXUS and SENTRI		Nine digit numbers for: GOES, NEXUS, FAST, and SENTRI
Global Type *This is the type of enrollment program (TWIC, HME, Trusted Traveler)	Identifies the DHS Program being verified	Required: Enter one of the following values for each entry. Input of these values must be exact.	CDL/HME
			TWIC
			GOES, NEXUS, FAST, and SENTRI
CDL State	State abbreviation	Required: When DHS program is CDL/HME	Must be U.S. Postal Service Alpha-2 code www.usps.com
Expiration Date	Expiration date for the program being selected for verification. Commonly known as the credential’s expiration date.	Required: For all Option 2 submissions	MM/DD/YYYY
Revert to Option One	If this submission should automatically revert to Option 1 under the system rules (refer to Section 4.1.2), then a value must be entered.	Required: All Option 2 submissions that are ‘Revert to Option 1’ must contain a ‘true’ in the value for each affected individual submitted	‘True’ value only
Custom Field ID	This field refers to the UDF ID number that is given after a UDF is created within the system	Optional: Must be a valid UDF that is accessible to the user on the affected individual’s record from within the system	Numbers only
Value	Value of UDF. This is the information applicable to the field for the user.	Optional: Can be number, letters and special characters. No longer than 200 characters.	There is no format for this field

Option 2 (Revert to Option 1) Bulk Upload - Field Mapping			
Field	**Description**	**Validation Rules**	**Format**
No Access Date	Date when affected individual will no longer have access to restricted areas or critical assets at a facility. Upon the specified date, the affected individual will no longer have access.	Optional: The date must be greater than today and less than 10 years from now	MM/DD/YYYY

Appendix C: Common User Management Scenarios

EXAMPLE 1: A CFATS covered facility, ACME Chemical, has hired ABC Security to conduct background checks on affected individuals that are employees of ACME Chemical.

QUESTION: What needs to happen to have information about the affected individuals that are employees of ACME Chemical submitted under Option 1 or Option 2 by ABC Security?

ANSWER: In the CSAT PSP application, the ACME Chemical Authorizer needs to create a group for ABC Security, create a PSP Submitter role for one employee of ABC Security, and then associate the PSP Submitter to the ABC Security group. The PSP Submitter can then submit information about the affected individuals that are ACME Chemical employees via Option 1 or Option 2. Note: Affected individuals submitted by ABC Security will automatically be added to the ABC Security group.

EXAMPLE 2: A corporation, which includes two CFATS-covered facilities, ACME Chemical and ACME Non-Traditional Chemical, has hired ABC Security to conduct background checks on affected individuals that are employees of the corporation. The corporation manages both CFATS covered facilities under a single Authorizer.

QUESTION: What needs to happen to have the information of the affected individuals that are employees at either ACME Chemical or ACME Non-Traditional Chemical submitted under Option 1 or Option 2?

ANSWER: The Authorizer has two alternatives.

ALTERNATIVE 1: Create a single group, then create a PSP Submitter role for one employee of ABC Security, and assign the ABC Security PSP Submitter to the group. The ABC Security PSP Submitter will be able to submit records about affected individuals from both facilities to the single group. This will allow information about affected individuals with access to either or both facilities to be submitted once.

ALTERNATIVE 2: Create two groups, then create an ABC Security PSP Submitter and associate it with the first group. Next, create a second PSP Submitter role and associate it to the second group. ABC Security can then use the different user roles to submit information about affected individuals to each respective group. This may result in some affected individuals' information being submitted more than once, but may align more closely with existing access control or background check processes already in place between each facility and its contractor.

EXAMPLE 3: ABC Security has been hired to conduct background checks on affected individuals at two separate CFATS-covered facilities (i.e., ACME Chemical and XYZ Chemical). The CFATS covered facilities are organized under different Authorizers within CSAT. Some affected individuals have access to both CFATS-covered facilities.

QUESTION: What needs to happen to have information about the affected individuals submitted correctly?

ANSWER: The Authorizers for ACME Chemical and XYZ Chemical will each need to create a group for ABC Security. Following the creation of the groups, the Authorizers for each facility will need to assign an employee(s) of ABC Security the PSP Submitter role for their respective group. Authorizers should consult with ABC Security to determine if employees of ABC Security already have existing PSP Submitters user roles.

If an affected individual has access to both covered facilities, the PSP Submitter for ABC Security will submit information about the affected individual twice, once on behalf of each facility. To accomplish this, ABC Security, using one of the PSP Submitter user roles, will need to login and submit information about the affected individual under the applicable option (Option 1 or Option 2). ABC Security can then either log out and then login under the other PSP Submitter user role or, if during registration the ABC Security PSP Submitter was registered as an existing CSAT user, the user can switch between authorizers using the ‘Switch Authorizers’ link that appears in the top right corner of the PSP application.

EXAMPLE 4: A CFATS covered facility, ACME Chemical, has multiple contracts with different companies (e.g., Landscape Inc. and Security Patrol Inc.). Each company providing a contracted service may employ people that meet the criteria as affected individuals, in accordance with ACME Chemical’s SSP or ASP.

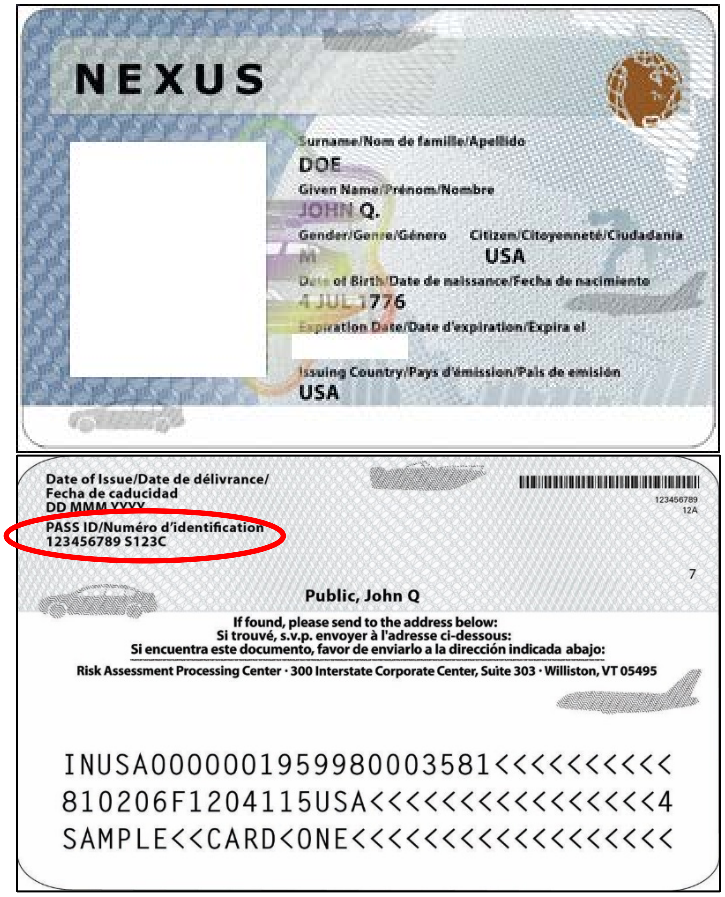
QUESTION: What needs to happen to have information about the affected individuals that are employees of Landscape Inc. and employees of Security Patrol Inc. submitted under Option 1 or Option 2?

ANSWER: The Authorizer for ACME Chemical has two alternatives for submitting information about affected individuals that are employees of Landscape Inc. and employees of Security Patrol Inc.

ALTERNATIVE 1: The Authorizer (or a PSP Submitter employed by ACME Chemical who is a member of the default group) may submit information about all affected individuals that are employees of Landscape Inc. and Security Patrol Inc. group. This option will render all submissions into the default group.

ALTERNATIVE 2: The Authorizer may create groups for both Landscape Inc. and Security Patrol Inc. Following the creation of these groups, the Authorizer will need to (1) create PSP Submitter accounts for both Landscape Inc. and Security Patrol Inc. and (2) associate the PSP Submitter for Landscape Inc. and the PSP Submitter for Security Patrol Inc. with their respective group. The PSP Submitters for Landscape Inc. and Security Patrol Inc. will then be able to submit information about affected individuals from their respective companies without viewing the SPII of each other’s employees.

Appendix D: Locating the Trusted Traveler Program Pass ID



NEXUS

Surname/Nom de famille/Apellido
DOE

Given Name/Prénom/Nombre
JOHN Q.

Gender/Genre/Género
M

Citizen/Citoyenneté/Ciudadania
USA

Date of Birth/Date de naissance/Fecha de nacimiento
4 JUL 1776

Expiration Date/Date d'expiration/Expira el

Issuing Country/Pays d'émission/País de emisión
USA

Date of Issue/Date de délivrance/
Fecha de caducidad
DD MMM YYYY

PASS ID/Numéro d'identification
123456789 S123C

123456789
12A

7

Public, John Q

If found, please send to the address below:
Si trouvé, s.v.p. envoyer à l'adresse ci-dessous:
Si encuentra este documento, favor de enviarlo a la dirección indicada abajo:

Risk Assessment Processing Center · 300 Interstate Corporate Center, Suite 303 · Williston, VT 05495

```
INUSA000000195998000358 1<<<<<<<<<<
810206F1204115USA<<<<<<<<<<<<<<<4
SAMPLE<<CARD<ONE<<<<<<<<<<<<<<<<<
```

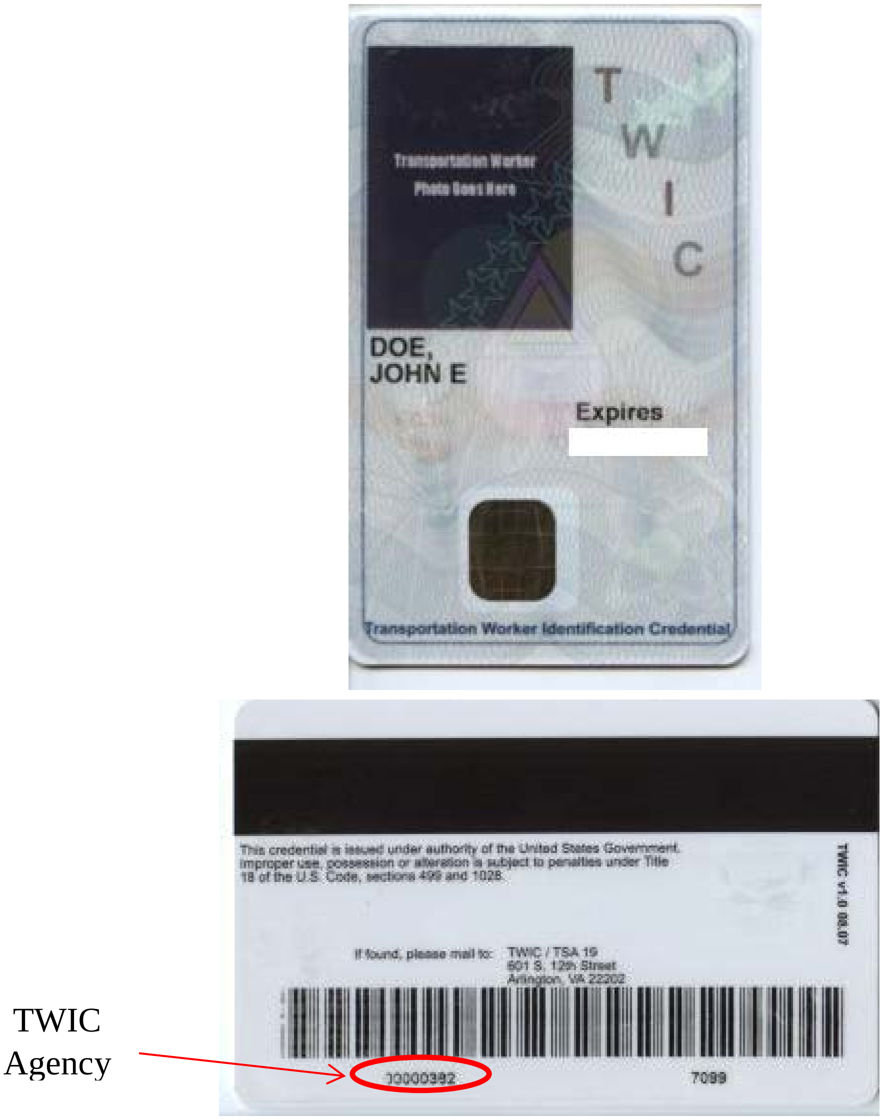
Figure 8: Trusted Traveler Program Pass ID

Appendix E: Locating the Agency Serial Number from a TWIC

Locating the TWIC Agency Serial Number from a TWIC issued before May 2014

The TWIC Agency Serial Number or Agency Serial Number (ASN) is displayed under the barcode on the back of the TWIC. It is composed of eight numeric characters. The ASN is also stored in the TWIC electronic chip as an element referred to as the Card Image Number (CIN).

Using the example below, the number that would be input into the PSP application in the TWIC ASN data field is 00000392.



This credential is issued under authority of the United States Government. Improper use, possession or alteration is subject to penalties under Title 18 of the U.S. Code, sections 499 and 1028.

If found, please mail to: TWIC / TSA 19
601 S. 12th Street
Arlington, VA 22202

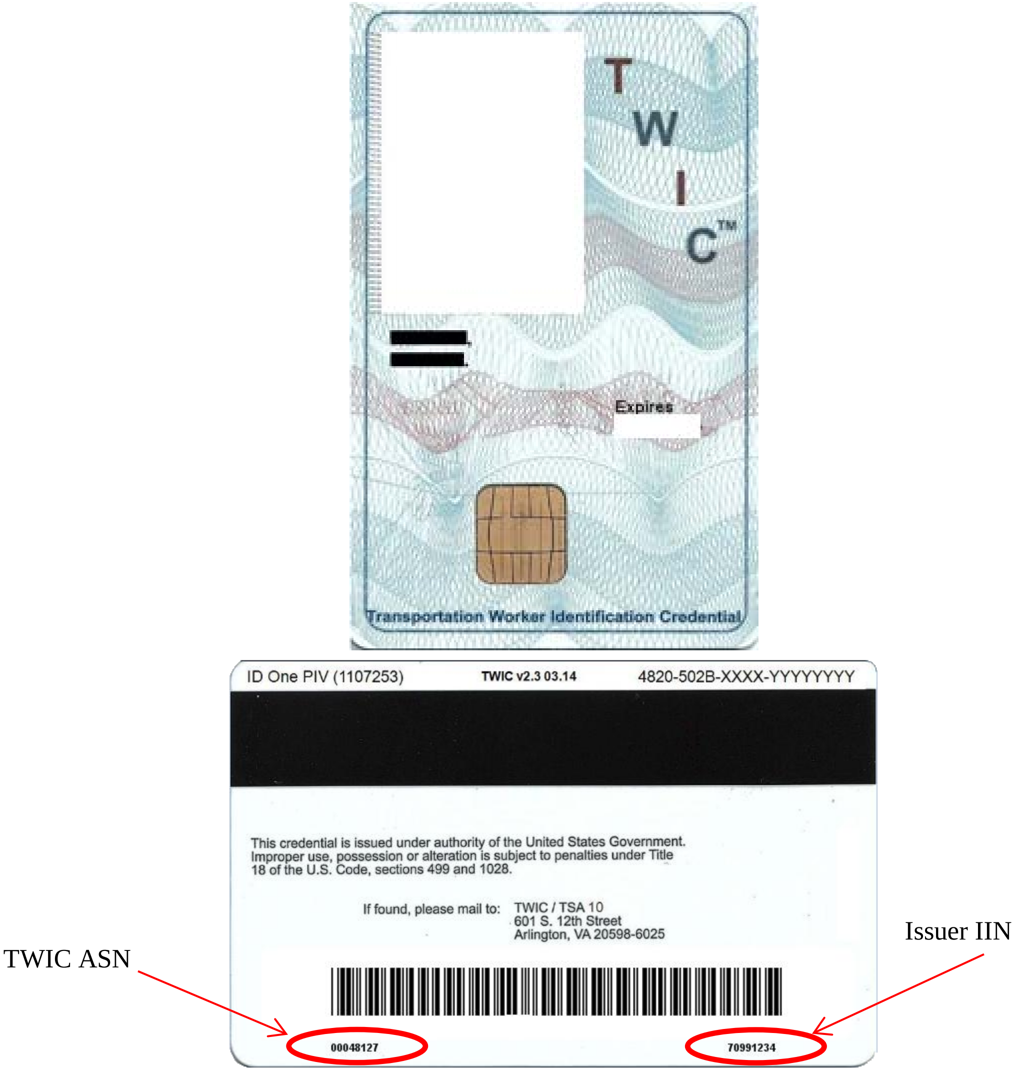
Figure 9: TWIC Agency Serial Number displayed on TWIC issued before May 2014

Locating the TWIC Agency Serial Number on a TWIC issued on or after May 2014

The TWIC Agency Serial Number is displayed under the barcode on the back of the TWIC. It is composed of eight numeric characters. As with cards issued before May 2014, the ASN is also stored in the TWIC electronic chip as an element referred to as the CIN.

When inputting the TWIC Agency Serial Number from a TWIC issued on or after May 2014 users must also add the Issuer Identification Number (IIN) to the beginning of the TWIC ASN. This series of numbers joined in this order is referred to as the Universal Credential Identification (UCI) Number.

Using the example below the, the number input into the PSP application in the TWIC ASN data field is 7099123400048127. This UCI is the IIN of 70991234 and the TWIC ASN is 00048127 joined together in the proper order.



This credential is issued under authority of the United States Government. Improper use, possession or alteration is subject to penalties under Title 18 of the U.S. Code, sections 499 and 1028.

If found, please mail to: TWIC / TSA 10
601 S. 12th Street
Arlington, VA 20598-6025

Figure 10: TWIC Agency Serial Number displayed on TWIC issued after May 2014

Electronically extracting the TWIC Agency Serial Number from a TWIC issued before or after May 2014

When the TWIC Agency Serial Number is electronically extracted either from the embedded chip or bar code, the actual number extracted is the UCI Number. This is true of TWICs issued before and after May of 2014.

When read from the barcode, the full UCI is available as output from the barcode scanner as a single 16-digit number. The IIN (Tag 0x42) and the CIN (Tag 0x45) can be separately read from the chip and joined together to construct the UCI. Both IIN and CIN can be freely retrieved by issuing a GET DATA command after selecting the card manager (AID -0xA0000001510000) using their respective tags.

The UCI should be used when inputting data into the TWIC Agency Serial Number data field within the PSP application.

For more information about how to electronically extract the UCI from TWICs, please refer to either (1) FIPS PUB 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013, which can be found at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=914530, or (2) the Global Platform Specification Version 2.2.1, January 2011, which can be found at http://www.globalplatform.org/specificationscard.asp.

Appendix F: CFATS PSP Policy Statements

Submitting an affected individual's full name under Option 1

A facility or its designee(s) must submit the affected individual's full name. This includes an affected individual's first name, middle name, last name, and any other known suffix such as "Jr." or "III." The CSAT PSP application will accept a facility's submission if the affected individual's name does not contain a middle name or a suffix because some people do not have a middle name or suffix. If an affected individual has a middle name or suffix, then a facility is required by policy (not IT validation rules) to submit that information.

How to treat an affected individual with dual citizenship under Option 1

If the affected individual has dual citizenship, of which one is U.S. citizenship, treat the affected individual as if they were only a U.S. citizen. It is not required to insert the other citizenship the affected individual enjoys.

If the affected individual has dual citizenship, and neither is U.S. citizenship, you may select either citizenship to submit.

Submitting optional information under Option 1 to reduce the likelihood of false positives

While the Department will accept, under Option 1, the submission of an affected individual's information that meets the minimum requirements, the Department strongly encourages facilities and their designee(s) to submit the requested optional data elements (i.e., alias(es), gender (for non-U.S. Persons), and place of birth) to reduce the likelihood of false positives. The inclusion of an affected individual's Redress Number is particularly helpful because the Redress Number was issued to the affected individual to assist with previous events that possibly involved misidentification.

Submitting both citizenship and gender under Option 1 to reduce the likelihood of false positives

While the Department will accept, under Option 1, the submission of an affected individual (if they are a U.S. Person) with either just gender, or just citizenship, the Department strongly encourages facilities and their designee(s) to submit both data elements to reduce the likelihood of false positives.

Submitting both Passport Information and Alien Registration Number under Option 1 to reduce the likelihood of false positives

While the Department will accept the submission of an affected individual (if they are a non-U.S. Person) with either just their Passport Information or just their Alien Registration Number, the Department strongly encourages facilities and their designee(s) to submit both data elements to reduce the likelihood of false positives.

Submitting an affected individual’s full name under Option 2

A facility or its designee(s) must submit the affected individual’s name that is displayed on the credential. Providing a full name other than what is displayed on the credential may result in the Department being unable to verify the affected individual’s enrollment via the CSAT PSP application. Trusted Traveler members who do not have a card can find their PASS ID, including the name they used to enroll with the trusted Traveler program, on their online GOES account at http://www.cbp.gov/travel/trusted-traveler-programs.

Submitting, under Option 2, optional information about affected individuals to the Department to reduce the potential for misidentification

While the Department will accept, under Option 2, the submission of an affected individual’s information that meets the minimum requirements, the Department strongly encourages facilities and their designee(s) to submit the requested optional data elements (i.e., alias(es), gender, place of birth, and citizenship) to reduce the likelihood of misidentification.

How to treat an affected individual who has dual citizenship under Option 2

Submission of citizenship information is optional under Option 2. If a facility submits optional citizenship information, the following guidance applies:

- If the affected individual has dual citizenship, of which one is U.S. citizenship, treat the affected individual as if they were only a U.S. citizen.
- If the affected individual has dual citizenship, and neither is U.S. citizenship, you may select either citizenship to submit.

Submitting updates and corrections under Option 1 or Option 2

Section 2102(d)(2)(A)(i) of the Homeland Security Act prohibits the Department from requiring a high-risk chemical facility to submit information about an individual more than one time under Option 1 or Option 2. Therefore, under Option 1 or Option 2, a high-risk chemical facility may choose whether to submit data updates or corrections about affected individuals.

The Department believes, however, that there are substantial privacy risks if a high-risk chemical facility opts not to provide updates and corrections (e.g., updating or correcting a name or date of birth) about affected individuals. Specifically, the accuracy of an affected individual's personal data being vetted against the TSDB for terrorist ties may be affected. Accurate information both (1) increases the likelihood of correct matches against information about known or suspected terrorists, and (2) decreases the likelihood of incorrect matches that associate affected individuals without terrorist ties with known or suspected terrorist identities. As a result, the Department encourages high-risk chemical facilities to submit updates and corrections as they become known so that the Department's checks for terrorist ties, which are done on a recurrent basis, are accurate. If a high-risk chemical facility is either unable or unwilling to update or correct an affected individual's information, the affected individual may seek redress as described in the CFATS PSP Privacy Impact Assessment.[3]

Multiple options to notify the Department that an affected individual no longer has access

Section 2102(d)(2)(A)(i) of the Homeland Security Act prohibits the Department from requiring a high-risk chemical facility to notify the Department when an affected individual no longer has access to the restricted areas or critical assets of a high-risk chemical facility. Therefore, under Option 1 or Option 2, a high-risk chemical facility has the option to notify the Department when the affected individual no longer has access to any restricted areas or critical assets, but such notification is not required. Nevertheless, the Department strongly encourages high-risk chemical facilities to notify the Department when an affected individual no longer has access to restricted areas or critical assets to ensure the accuracy of the Department's data and to stop the recurrent vetting on the person who is no longer an affected individual. If a high-risk chemical facility is either unable or unwilling to notify the Department when an affected individual no longer has access to restricted areas or critical assets, the affected individual may seek redress as described in the CFATS PSP Privacy Impact Assessment.

A facility or its designee may notify the Department that an affected individual no longer has access to restricted areas or critical assets (or that an affected individual will no longer have access to restricted areas or critical assets at some future time) in three possible ways:

1. Input a date the affected individual will no longer have access to restricted areas or critical assets in the PSP application. Records submitted with this field populated will automatically be removed upon the date provided. The date an affected individual will no longer have access can be updated as necessary. This is described in Section 4.1 for Option 1 and Section 4.2 for Option 2.

   POSSIBLE EXAMPLES USING THIS ALTERNATIVE:

   - A facility for which you are responsible may have scheduled a turnaround. When inputting the affected individual’s information, you may opt to input a date in this field for when the turnaround is scheduled to be completed.
   - A facility for which you are responsible may issue an access control badge that is valid for three years. You may opt to input the expiration date of that access control badge. You may then opt to update the date if the access control badge expiration date is changed.
   - For affected individuals granted access for only one day, it is acceptable to enter a date one day beyond the date the affected individual has and loses access.

2. Remove the group associated with the affected individual. This process is described in Section 6.9.
3. Manually remove the affected individual record. This process is described in Section 4.4.

[3] The original Privacy Impact Assessment for the CFATS PSP, published in 2011, and its subsequent updates are available at http://www.dhs.gov/publication/dhs-nppd-pia-018a-chemical-facilities-anti-terrorism-standards-personnel-surety.

When the Department is notified through one of the actions above that an affected individual no longer has access to restricted areas or critical assets, the record will no longer be displayed as a part of the Group. The Department will also (1) stop vetting the affected individual in accordance with the record retention schedule[4] if the affected individual was submitted under Option 1, or (2) stop verifying the affected individual's enrollment in other DHS programs.

[4] The CFATS PSP SORN, available at https://www.federalregister.gov/articles/2014/05/19/2014-11431/privacy-act-of-1974-department-of-homeland-security-national-protection-and-programs-directorate-002#p-103, describes the record retention schedule.